4 最適化のスケジュール

NTFS ファイルシステムでは、ファイルを１つまたは２つ以上のクラスタに保存します。クラスタはディスクの最小のデータアロケーション単位です。NTFS では、可能であれば連続したクラスタにファイルを書き込みますが、そうでない場合は分割して書き込みます。

その状態を「断片化」と呼びます。断片化が進むとファイルアクセスが遅くなるため、連続した領域に配置しなおす必要があります。これを「最適化」と呼び、Windows Storage Server 2003 より、WebUI のメニューから実行できるようになりました。この章では、スケジュールを設定して、毎日、毎週、毎月のいずれかのタイミングで iStorage NS 上のディスクを最適化する方法について説明します。

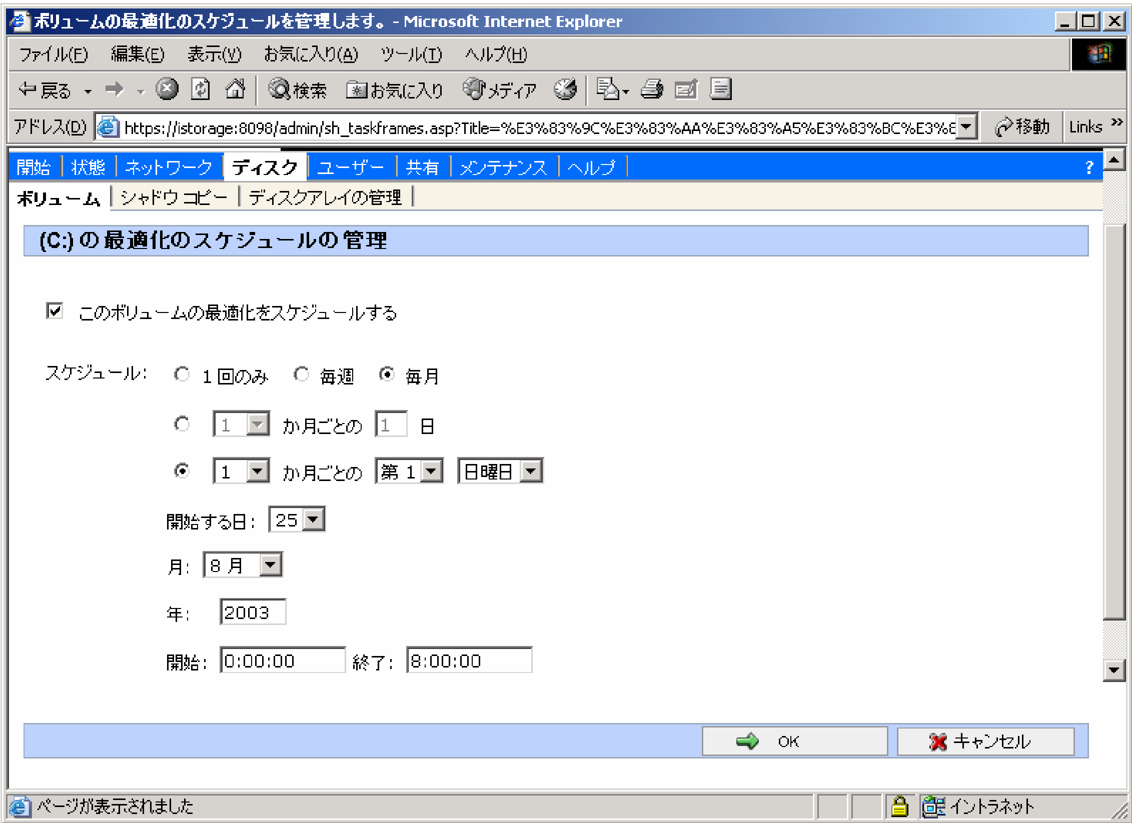
4.1　概要

最適化のスケジュールとはデフラグのスケジュール設定、及び実行を行う機能です。ボリューム毎に設定を行う事が可能です。スケジュール形態を“1回のみ”、“毎週”、“毎月”の中から選んで設定を行います。

4.2　操作手順

以下に WebUI での操作手順を記述します。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します。
2. WebUI の[ディスク]→[ボリューム]をクリックします。
3. ボリュームのリストからボリュームを選択し、[最適化のスケジュール]タスクを選択します。
   “このボリュームの最適化をスケジュールする”のチェックをオンにすると下記画面が表示されますので、“1回のみ”、“毎週”、“毎月”の中から選択し、詳細な設定を行います。
4. 時刻の設定は 12 時間形式での設定も可能です。



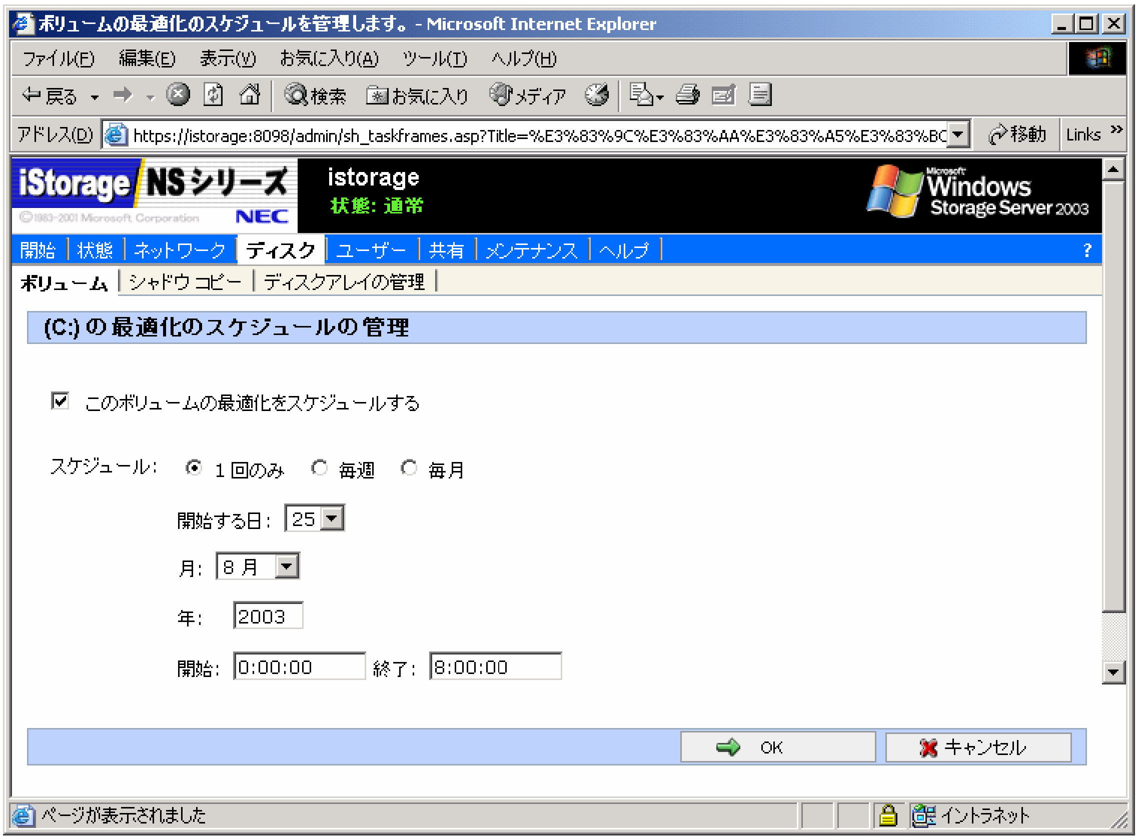
4.2.1　スケジュール設定（1 回のみ）

1 回のみの実行を行います。

以下に設定手順を記述します。

1. デフラグを開始する年月日を設定します。
2. “開始”と“終了”に開始時刻と終了時刻を入力します。
3. OK ボタンを押して設定完了です。

> デフラグの状況によっては“終了”時刻よりも早く終わる場合があります。



4.2.2　　スケジュール設定（毎週）

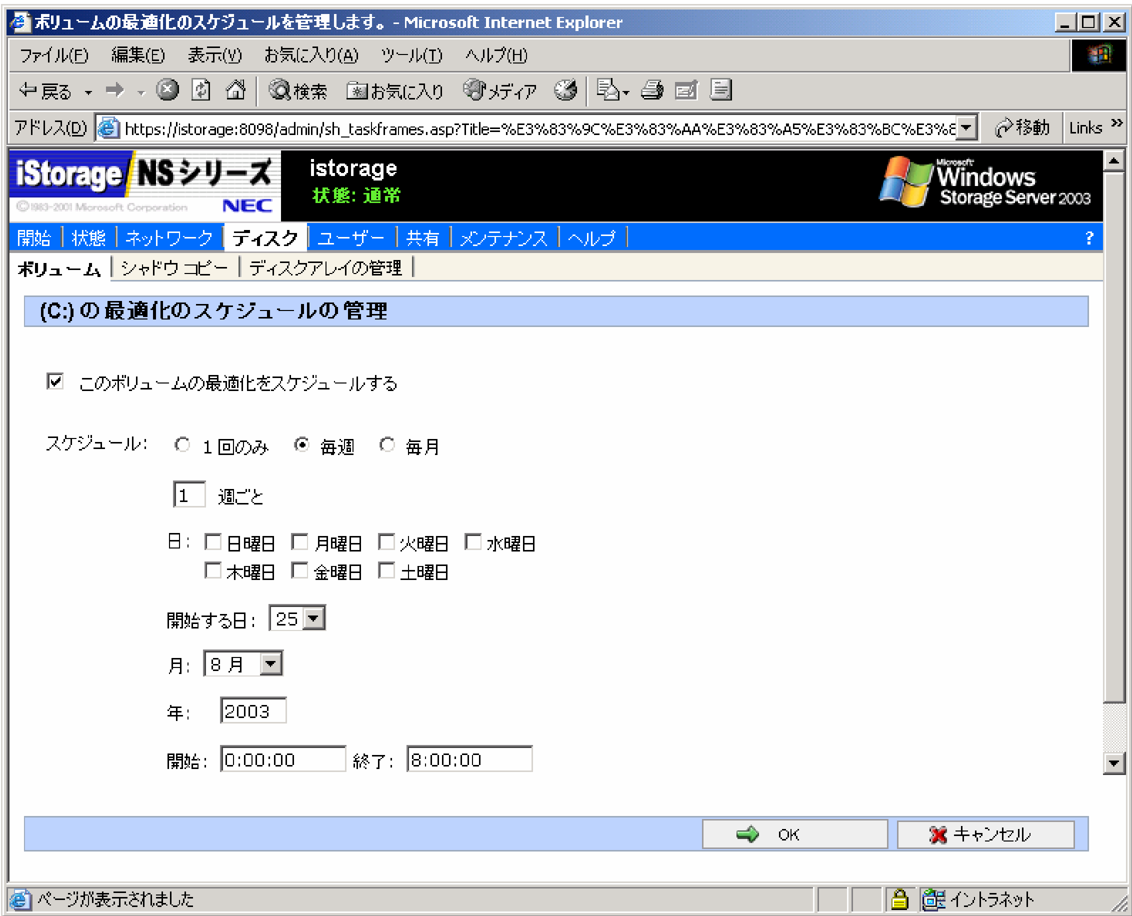
週単位での設定を行います。

毎週の実行だけでなく、数週間おきの実行スケジュールも設定可能です。

以下に設定手順を記述します。

1. 何週間おきの実行か入力します。1～52 の範囲で入力します。
2. デフラグを実行する曜日にチェックを付けます。複数選択可能です。
3. デフラグを開始する年月日を選択します。
4. “開始”と“終了”に開始時刻と終了時刻を入力します。
5. OK ボタンを押して設定完了です。

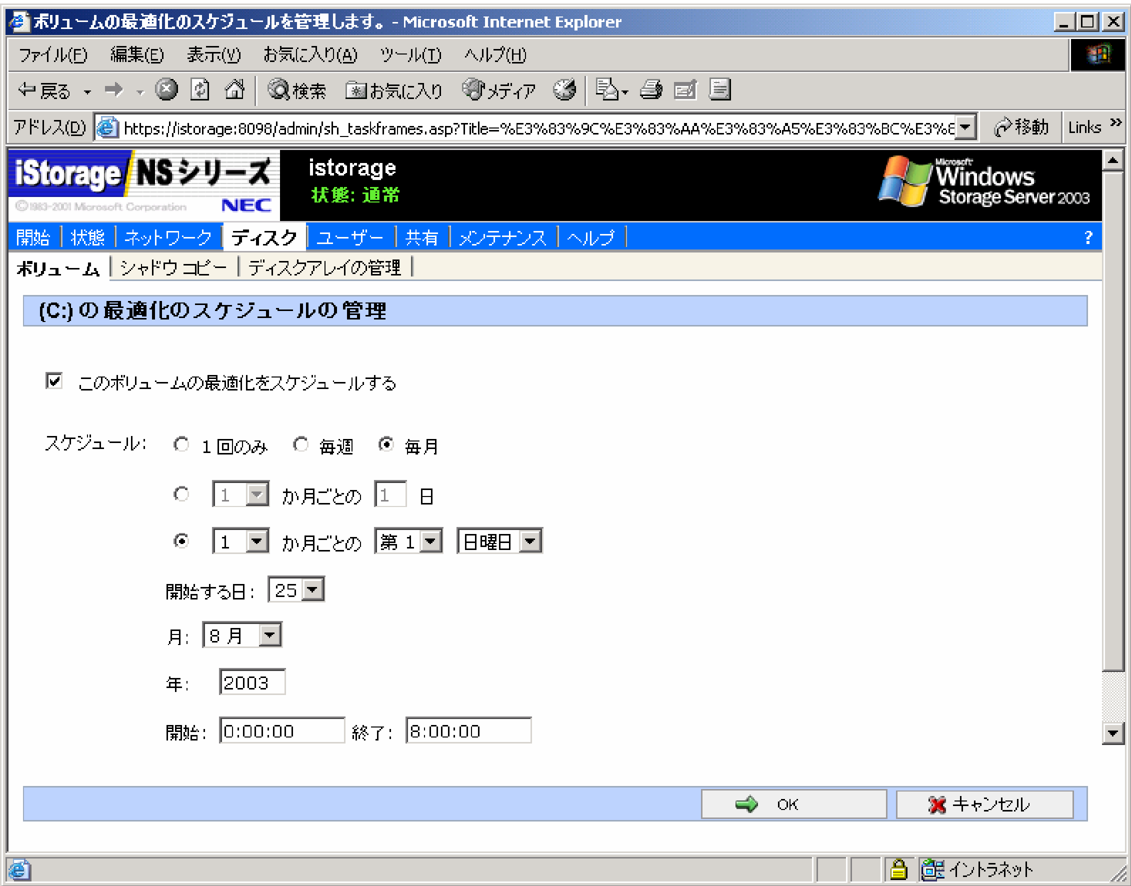
> デフラグの状況によっては“終了”時刻よりも早く終わる場合があります。
> ここで設定したスケジュールが有効になるのは上記 3)で設定した日付以降です。



4.2.3　　スケジュール設定（毎月）

月単位での設定を行います。毎月の実行だけでなく、数カ月おきの実行スケジュールも設定可能です。以下に設定手順を記述します。

1. デフラグの実行日が決まっている場合、その日付を入力し、何ヶ月おきに実行を行うのか、“１、２、３、４、６、１２”の中から選択します。
   また、日付でなく曜日で設定する場合は、曜日を“日曜 ～ 土曜”から選択し、月の第何週なのかを“第１、第２、第３、第４、最終”から選択します。
   何ヶ月おきの実行なのかも上記同様に設定します。
2. デフラグを開始する年月日を選択します。
3. “開始”と“終了”の後に開始時刻と終了時刻を入力します。
4. OK ボタンを押して設定完了です。



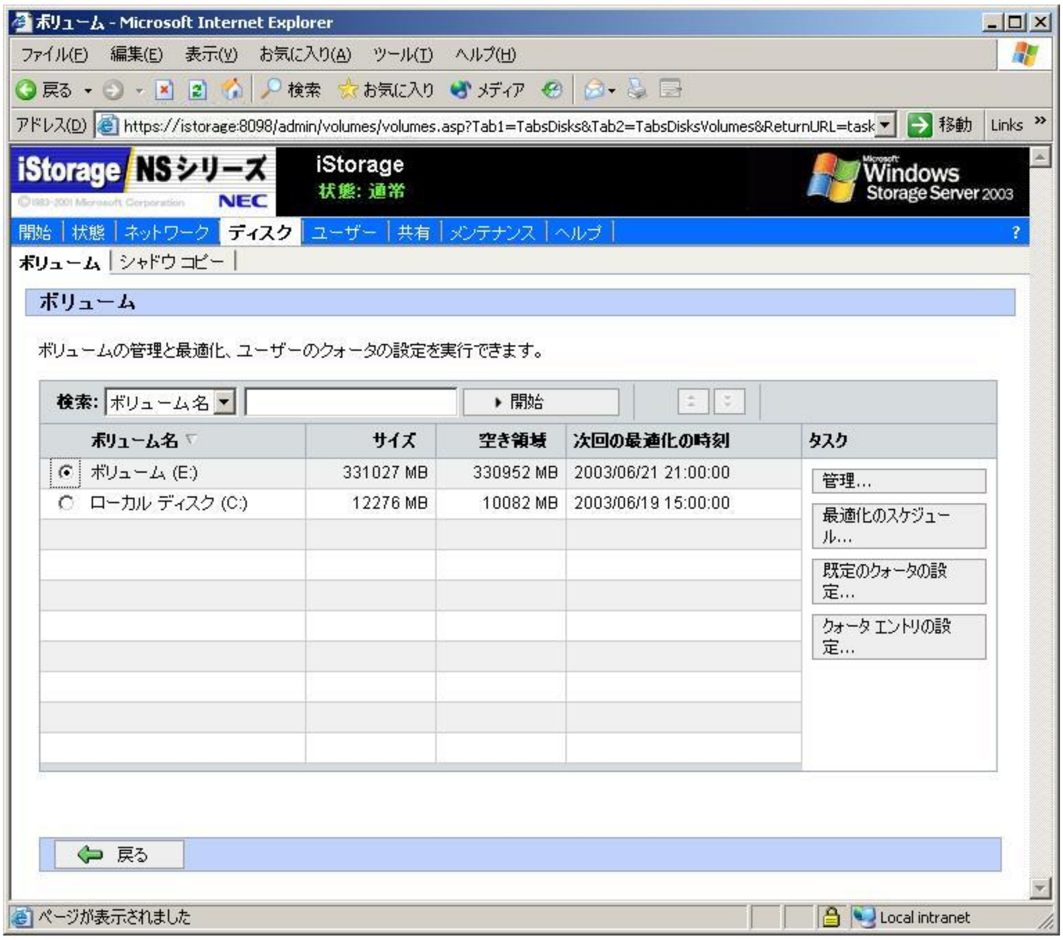
> デフラグの状況によっては“終了”時刻よりも早く終わる場合があります。
> ここで設定したスケジュールが有効になるのは上記 2)で設定した日付以降です。

4.3　設定スケジュールの確認

以下に操作手順を記述します。

1. WebUI の[ディスク]→[ボリューム]をクリックします。
2. スケジュールの設定により、次回の最適化の時刻が表示されます。
3. [最適化のスケジュール]よりスケジュールの再設定も行う事ができます。

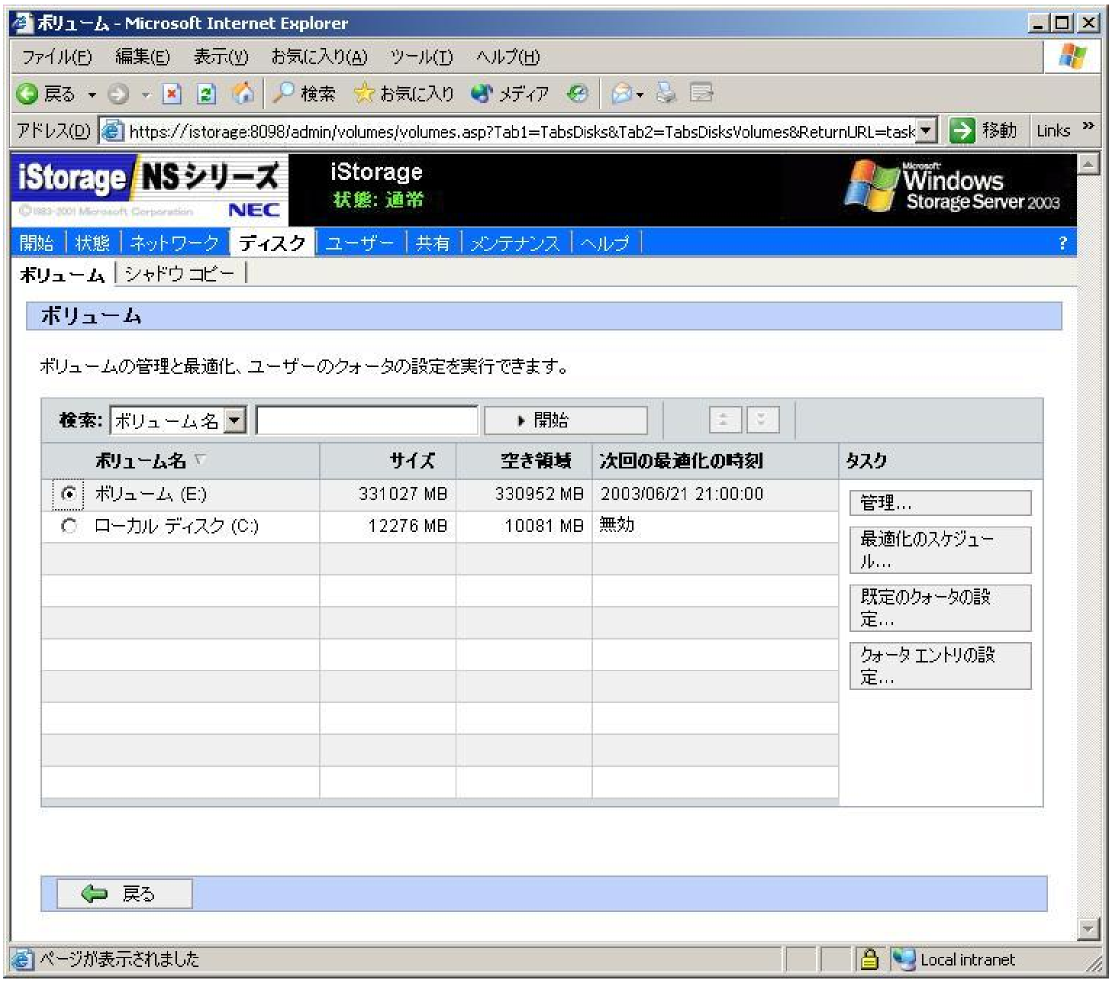
> スケジュールの設定はボリューム毎に一つまで設定できます。



4.4　デフラグ実行後の確認

以下に操作手順を記述します。

1. WebUI の[ディスク]→[ボリューム]をクリックします。
2. スケジュールが“1回のみ”の場合、デフラグが完了したボリュームは次回の最適化の時刻欄が“無効”になっています。
3. スケジュールが“1回のみ”以外の場合、次回の最適化の時刻が表示されています。



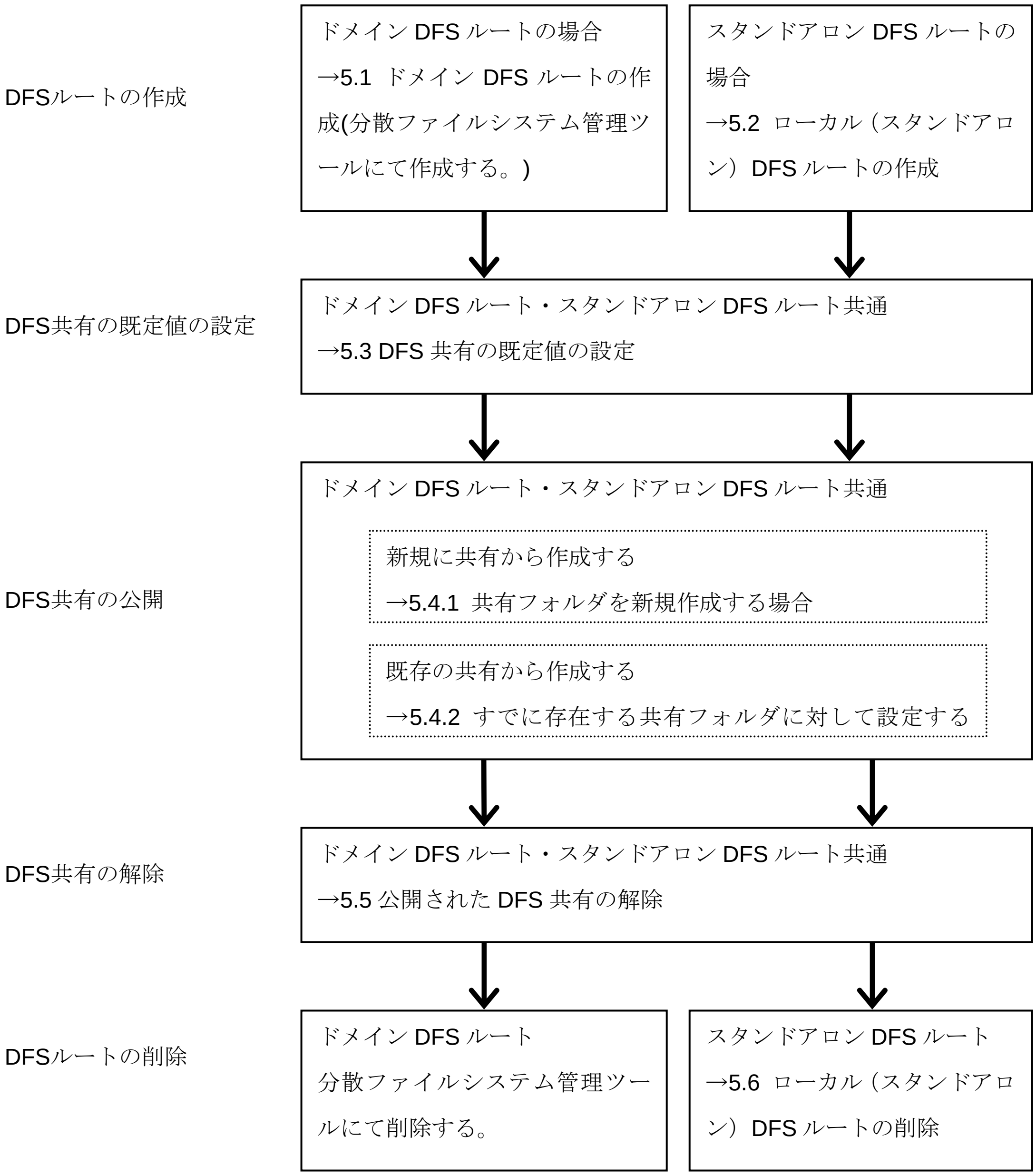
5 ファイル分散システム (DFS)

システム管理者が分散ファイルシステム(DFS)を使用すると、ネットワーク上に物理的に分散しているファイルへのアクセスと、それらのファイルの管理を簡単に行える環境をユーザーに提供できます。DFS では、複数のサーバーに分散しているファイルが、ネットワーク上の 1 つの場所に配置されているように見えます。ユーザーは、ファイルの物理的な場所を指定しなくても、目的のファイルにアクセスできます。

WebUI では、スタンドアロンルートの分散ファイルシステムのみをサーバー上に作成できます。ドメイン分散ファイルシステムや、他のサーバー上のスタンドアロンルート分散ファイルシステムを作成することはできません。ただし、どちらの種類の分散ファイルシステムを使用しているフォルダでも共有できます。

> ドメイン DFS ルートの作成または複数のルートを作成する場合、複数のルートが存在する環境で DFS 共有を公開する場合は、リモートデスクトップで iStorage NS にログオンし、管理者メニューより「分散ファイルシステム」を選択し「起動」ボタンをクリックしてください。分散ファイルシステム管理ツールが起動します。ヘルプを参照して、操作してください。

DFS(分散ファイルシステム)共有の操作の流れ



5.1　ドメインDFSルートの作成

WebUI を使用してドメイン DFS ルートは作成できません。ドメイン DFS ルートを作成するには、分散ファイル システム管理ツールを使用する必要があります。詳細については、Windows 2000/2003 のヘルプを参照してください。iStorage NS で作成可能なドメイン DFS ルートは１つのみです。

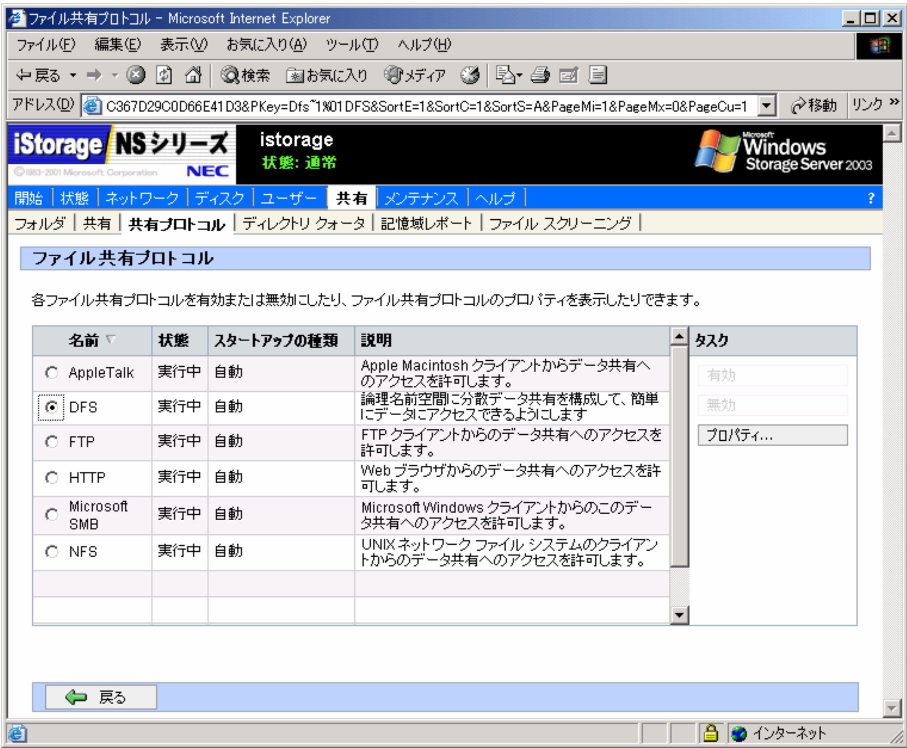
5.2　ローカル（スタンドアロン）DFSルートの作成

WebUI を使用して、ローカルスタンドアロン DFS ルートをサーバー上に１つ作成できます。

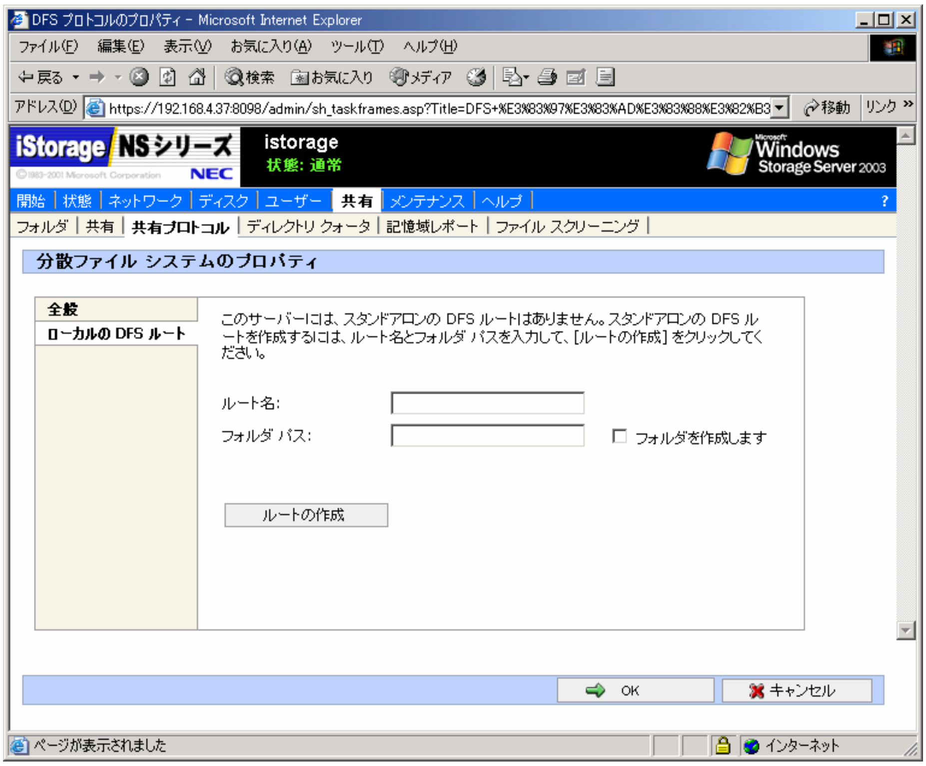
複数のローカルスタンドアロン DFS ルートを作成する場合は、リモートデスクトップで iStorage NS にログオンし、管理者メニューより[分散ファイルシステム]を選択し、[起動]ボタンをクリックしてください。分散ファイルシステム管理ツールが起動します。ヘルプを参照して、作成してください。

以下に、WebUI を使用してローカルスタンドアロン DFS ルートを作成する手順を示します。

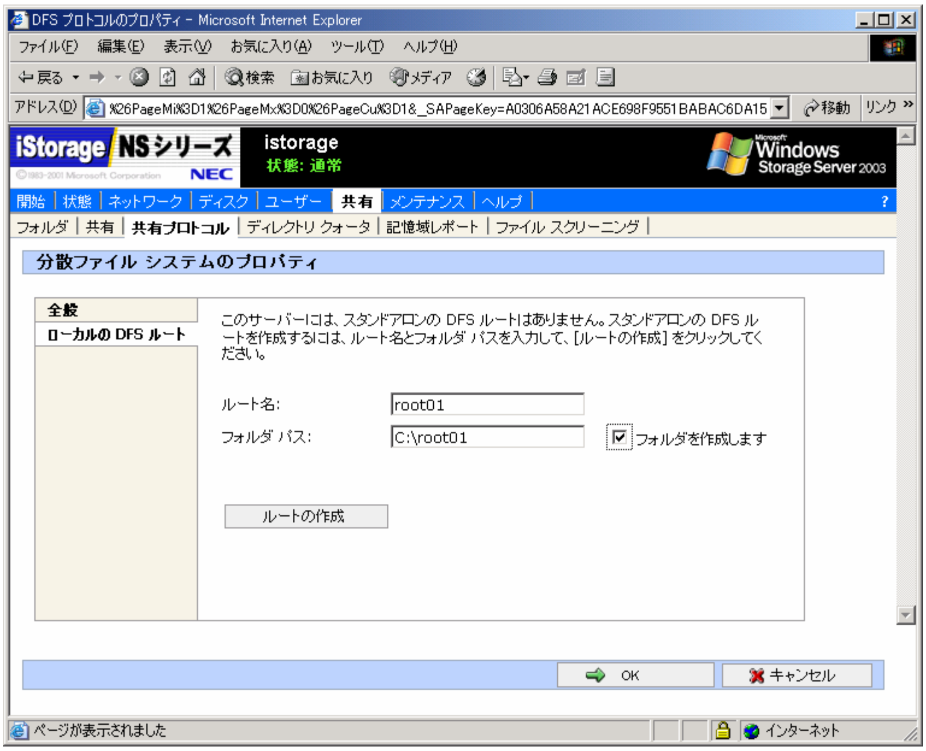
1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を起動します。
2. [共有]→[共有プロトコル]をクリックします。
3. [DFS]を選択し、[タスク]ボックスの[プロパティ]をクリックします。



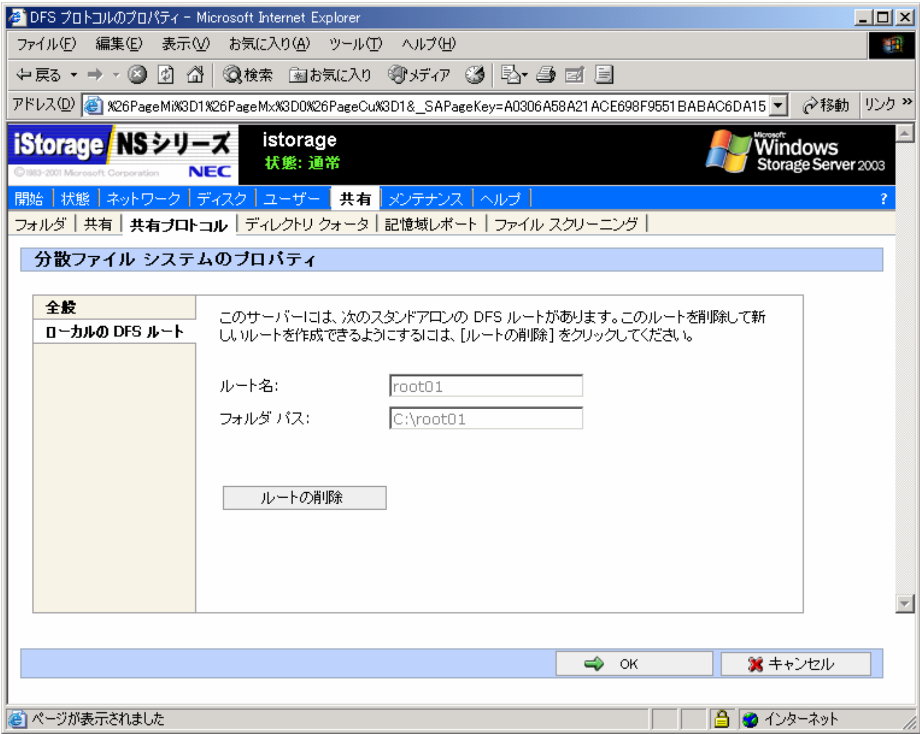
4. [分散ファイルシステムのプロパティ]が表示されます。[ローカルの DFS ルート]タブをクリックし、[ルート名]ボックスにローカルスタンドアロン DFS ルートの名前を入力します。



5. [フォルダ パス]ボックスに、ルートに対応するフォルダのパスを入力します。フォルダが存在しない場合は、[フォルダを作成します]にチェックを入れます。



6. [ルートの作成]をクリックします。[ルート名]、[フォルダ パス]の表示内容が、グレーに変わります。[OK]をクリックします。



「ルートの作成」をクリックしないと、DFS ルートは作成されません。「ルートの作成」をクリックせずに「OK」をクリックすると、共有プロトコル画面に戻り、入力したルート名・フォルダパスはクリアされます。

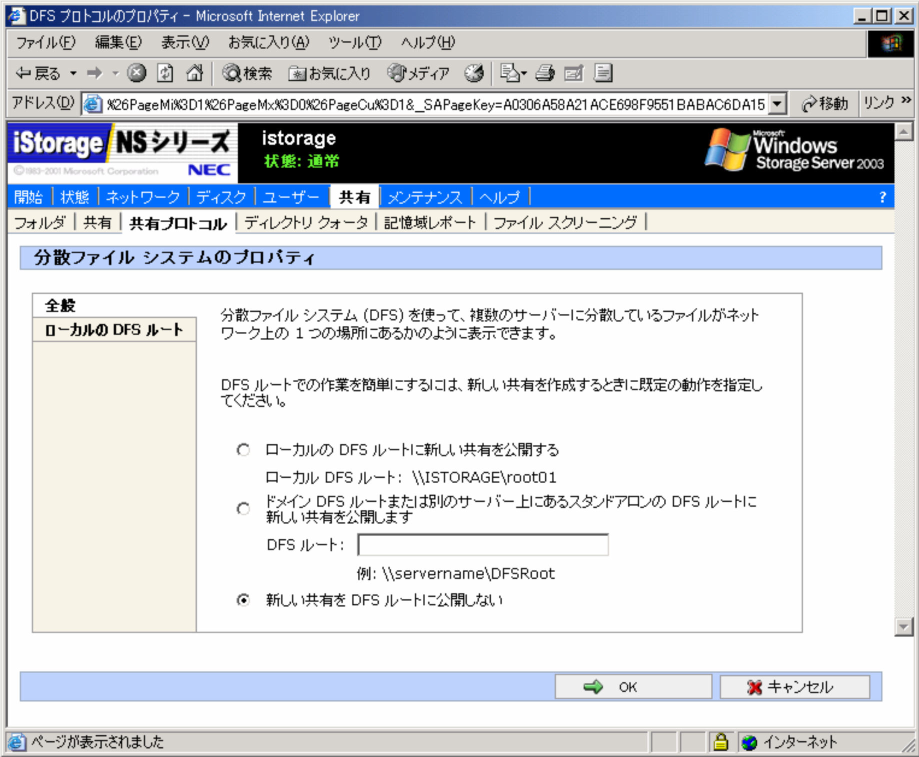
共有フォルダを DFS のルートに設定した場合、WebUI の「共有」→「共有」で表示される共有の一覧に表示されなくなります。DFS ルートを削除して、通常の共有に戻すと、共有の一覧に表示されるようになります。

5.3 DFS 共有の既定値の設定

WebUI を使用すると、共有フォルダの作成時に既定値として表示される DFS ルートを指定できます。新しい共有フォルダを作成するときに、ルートの設定が簡略化されます。また、既定値を設定しても、共有の公開を行う際、既定値に設定した以外のルートも指定できます。

1. WebUI の[共有]→[共有プロトコル]をクリックします
2. [ファイル共有プロトコル]画面が表示されます。

3. [DFS]を選択し、[タスク]ボックスの[プロパティ]をクリックします。
4. [全般]タブをクリックし、共有ディレクトリの作成時に使用する既定の設定を選択します。



- 共有をローカルスタンドアロン DFS ルートに公開するように既定値を設定するには、[ローカルの DFS ルートに新しい共有を公開する]を選択します。

> ローカルのスタンドアロン DFS ルートが設定されていない場合は、選択できません。

- 共有を別の DFS ルートに公開されるように既定値を設定するには、[ドメイン DFS ルートまたは別のサーバー上にあるスタンドアロンの DFS ルートに新しい共有を公開します]を選択します。[DFS ルート]ボックスに、既定値として設定する DFS ルートのパスを入力します。
- 共有を DFS ルートに公開しない場合は、[新しい共有を DFS ルートに公開しない]を選択します。

5. [OK]をクリックします。

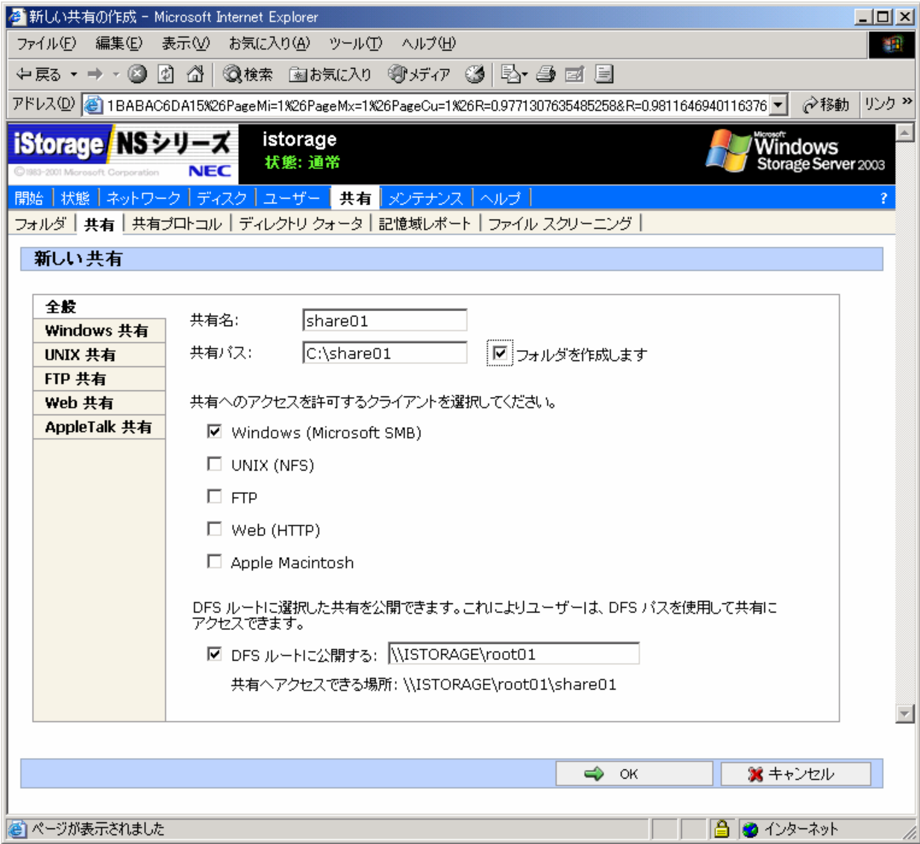
5.4 DFS での共有の公開

共有フォルダを DFS で公開するには、DFS ルートを指定する必要があります。

設定は以下の手順で行います。共有の公開には 2 通りの方法があります。共有フォルダを新規作成する際に設定する方法と、すでに存在する共有フォルダに対して設定する方法があります。

5.4.1　共有フォルダを新規作成する場合

1. WebUI の[共有]→[共有]をクリックします 。
2. [タスク]ボックスの[新規]をクリックします。

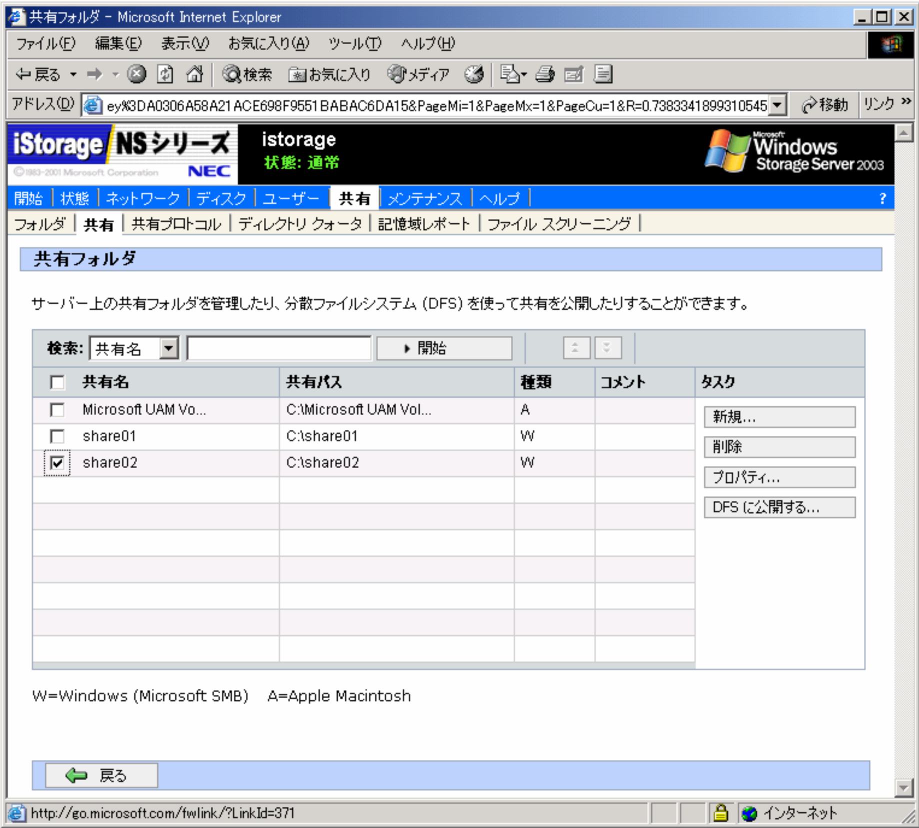


3. [新しい共有]画面が表示されますので、共有名・共有パスを入力します。フォルダが存在しない場合は、[フォルダを作成します]にチェックを入れます。
4. [共有へのアクセスを許可するクライアントを選択してください]の中から、Windows(Microsoft SMB)にチェックを入れます。
5. [DFS ルートに公開する]にチェックを入れます。
6. テキストボックスに、DFS ルートの名前を入力し[OK]をクリックします。DFS 共有の既定値を[共有を公開する]ように設定している場合は、パスが表示されます。これで構わない場合は、そのまま[OK]をクリックします。別のルートにする場合は、パスを入力し、[OK]をクリックします。

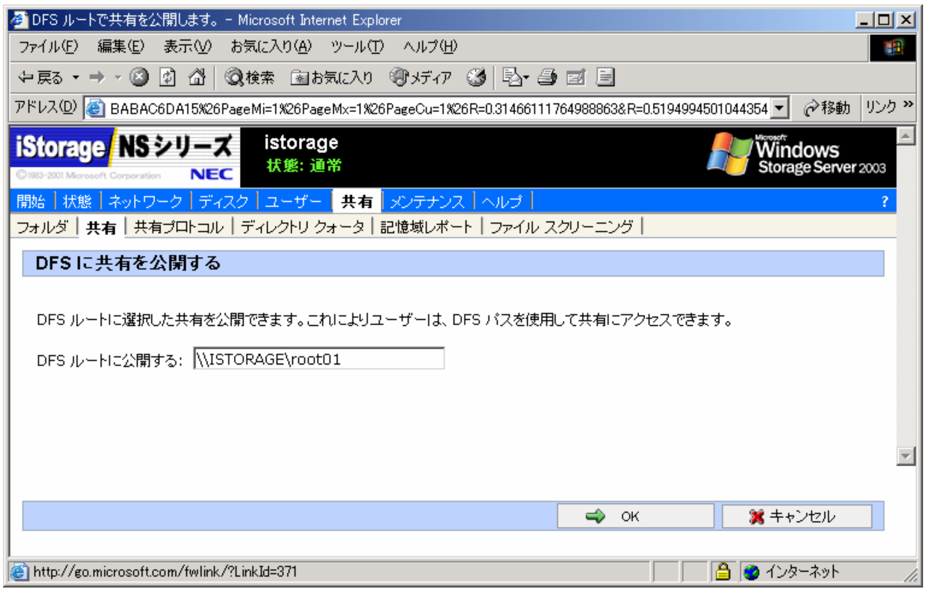
> 共有フォルダの新規作成の際に、Windows 共有(SMB)以外のプロトコルのみで共有を設定しても、DFS への共有の公開が設定できます。しかし、Windows 上の DFS 管理ツールや、マイネットワーク上に共有フォルダが表示されますが、実際にアクセスはできません。

5.4.2　すでに存在する共有フォルダに対して設定する場合

1. WebUI の[共有]→[共有]をクリックします。
2. DFS に共有を公開する共有フォルダにチェックを入れます。



3. [タスク]ボックスの[DFS に公開する]をクリックします。

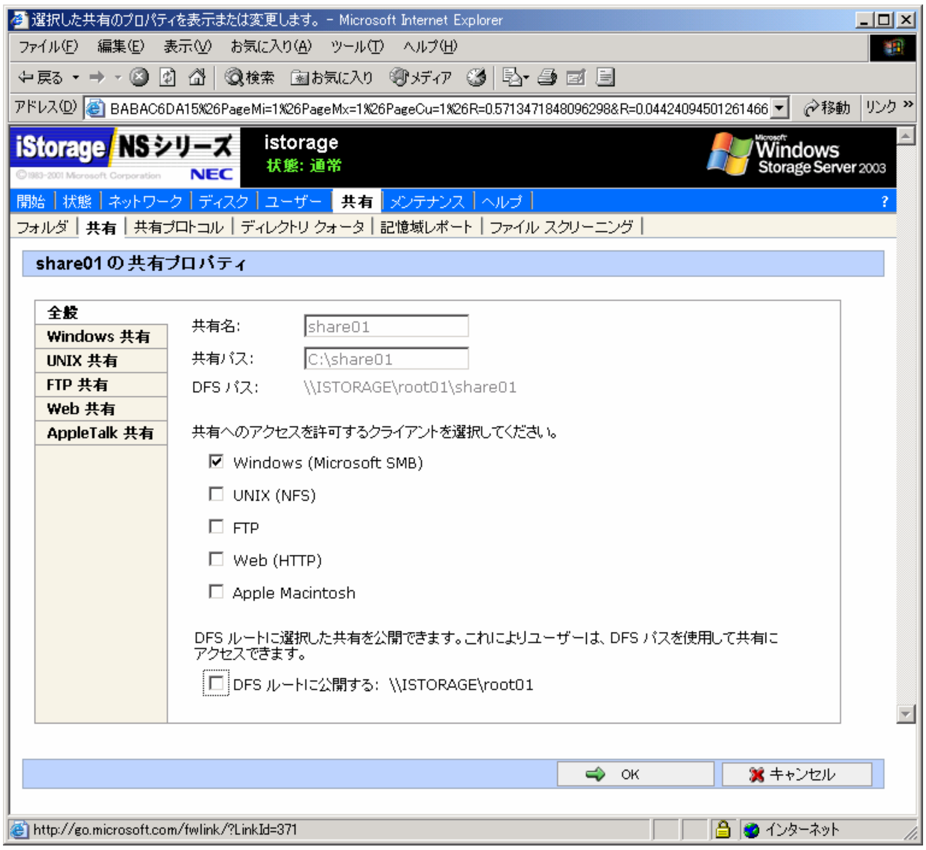


4. [DFS ルートに公開する]ボックスに、DFS ルートの名前を入力します。DFS 共有の既定値を[共有を公開する]ように設定している場合は、パスが表示されます。
5. これで構わない場合は、そのまま[OK]をクリックします。別のルートにする場合は、パスを入力し、[OK]をクリックします。

5.5　公開されたDFS共有の解除

一度公開した DFS 共有を解除する事ができます。これは、共有の公開が解除されるだけで、DFS ルートや共有フォルダの設定は変更されません。再度共有の公開が必要な場合は、「5.4 DFS での共有の公開」を参照して、設定してください。

1. WebUI の[共有]→[共有]をクリックします
2. DFS 共有を解除する共有フォルダにチェックを入れます。
3. [タスク]ボックスの[プロパティ]をクリックします。
4. プロパティ画面が表示されます。[DFS ルートに公開する]のチェックを外します。



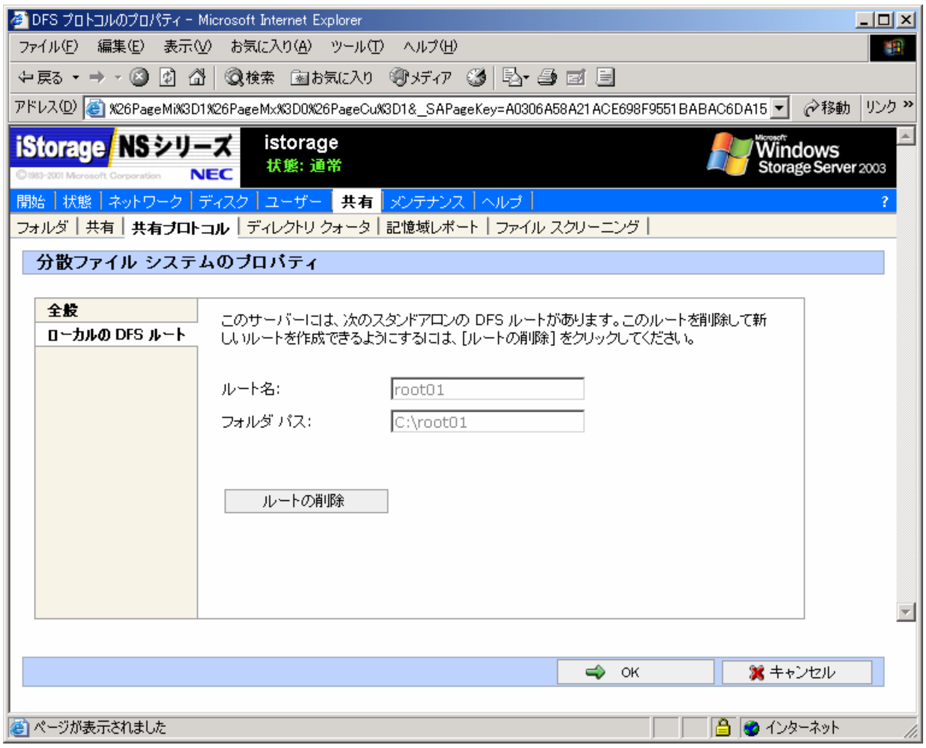
5. [OK]をクリックします。

5.6　ローカル（スタンドアロン）DFSルートの削除

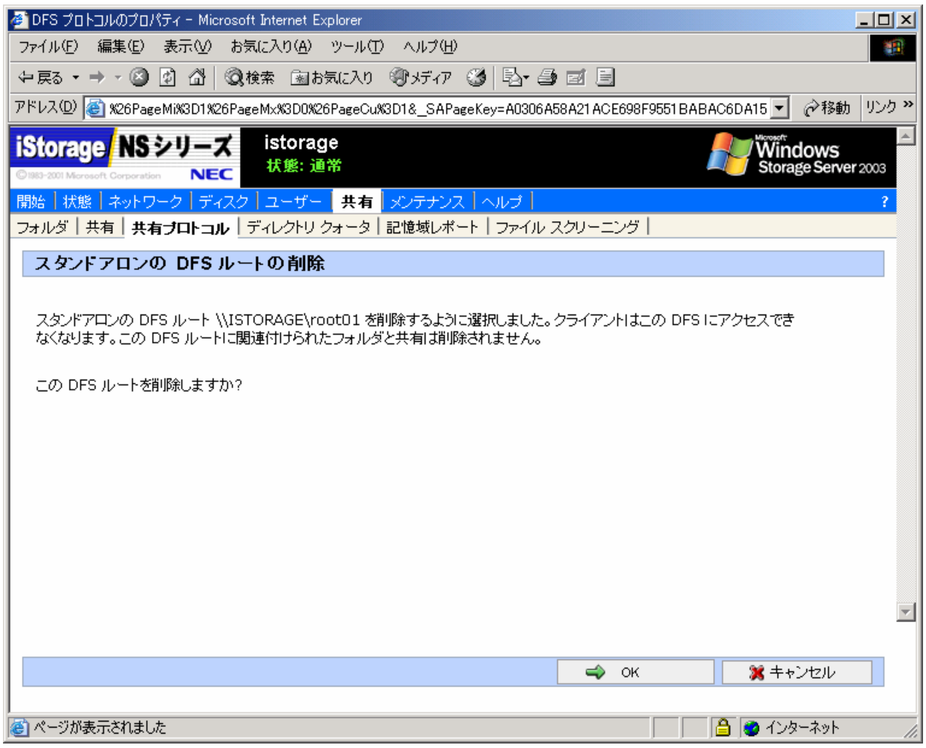
WebUI を使用して、サーバー上のローカル スタンドアロン DFS ルートを削除できます。

ローカルスタンドアロンの DFS ルートが複数存在する場合、最初に設定したルートが表示されます。特定の DFS ルートを選択して削除することはできません。リモートデスクトップで iStorage NS にログオンし、管理者メニューより[分散ファイルシステム]を選択し、[起動]ボタンをクリックしてください。分散ファイルシステム管理ツールが起動します。ヘルプを参照して、削除してください。

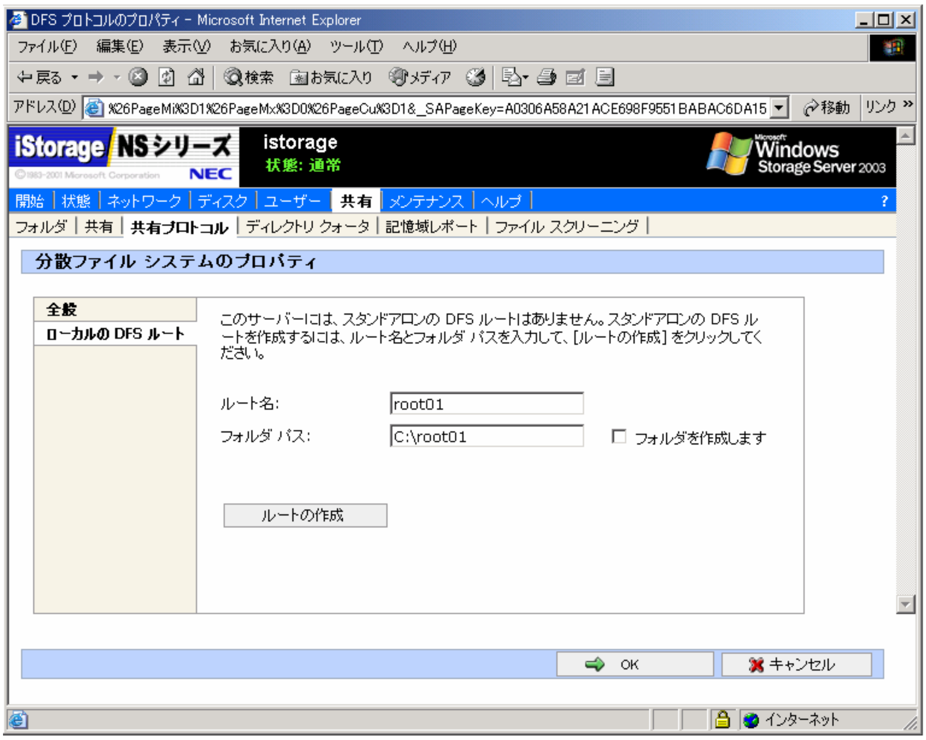
1. WebUI の[共有]→[共有プロトコル]をクリックします。
2. [DFS]を選択し、[タスク]ボックスの[プロパティ]をクリックします。
3. [ローカルの DFS ルート]タブを選択し、[ルートの削除]ボタンをクリックします。



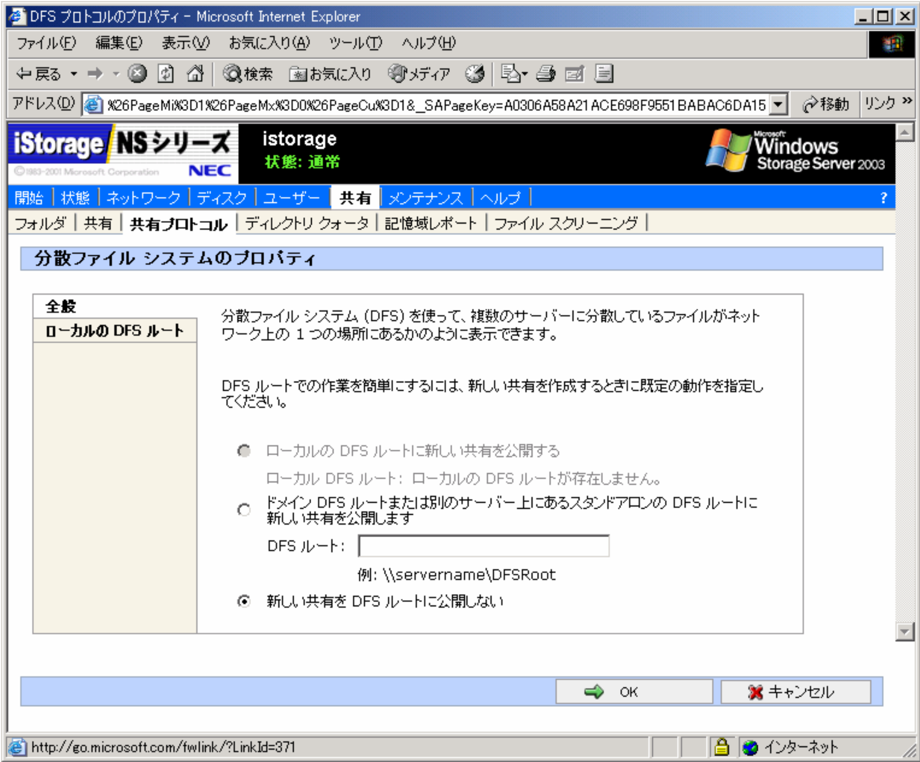
4. 確認メッセージ画面が表示されます。[OK]をクリックします。



5. [ルート名]、[フォルダ パス]の表示内容が、黒文字(入力可能状態)に変わり、[ルートの削除]ボタンが[ルートの作成]に変わります。[OK]をクリックします。



6. [分散ファイルシステムのプロパティ]画面の[ローカルの DFS ルートに新しい共有を公開する]がグレー表示になることを確認してください。



共有フォルダを一度 DFS ルートに設定し、共有を公開した後、DFS ルートを先に削除した場合、共有を公開されていたフォルダや共有の設定は残ります。また、一度 DFS ルートを解除した共有フォルダを再度 DFS ルートに設定する場合は、共有を削除する必要があります。WebUI の「共有」→「共有」で DFS ルートとなっていた共有名を選択し、タスクの「削除」で削除します。削除完了後、DFS ルートを作成します。

(一度 DFS ルートを解除した共有を DFS ルートに設定しようとすると、「DFS ルートの Microsoft SMB 共有を作成できません。DFS ルートと同じ名前の共有が存在しないことを確認して、再試行してください。問題が解決しない場合は、Windows Management サービスを再起動してください。」のエラーが表示され、設定できません。)

6 シャドウコピー

シャドウコピーサービスは、ある時点でのボリュームのコピーを作成し、保存しておく機能です。このコピー(シャドウコピー)を利用して、ユーザーは、ファイルやディレクトリを誤って削除した場合などに、以前の状態に戻すことができます。

シャドウコピーサービスはスケジューリング機能を持っているため、ご使用の環境やファイルの利用方法などに基づいてシャドウコピーの作成をスケジューリングし、一定のタイミングで自動的にシャドウコピーを作成することができます(毎日 5:00AM など)。ユーザーがサーバ上に保存しているファイルを誤って削除した場合や誤って更新した場合などに、ユーザーはシャドウコピーサービスを利用してそれらのファイルやディレクトリをシャドウコピー作成時の状態に戻すことができます。

サーバ上のファイルを元の状態に戻す場合、管理者が復元操作を行う必要はありません。ユーザーが自分自身で、クライアントコンピュータからネットワーク共有したサーバ上のファイルやフォルダに対して操作を行うことができます。

6.1　シャドウコピーの動作

シャドウコピーサービスでは、ボリューム単位でシャドウコピーを作成します。つまり、ボリューム上の特定の共有フォルダやファイルに対してのみシャドウコピーを作成するようなことはできません。しかし、復元する場合は、特定のフォルダやファイルのみを復元することができます。シャドウコピーは、最後に作成されたシャドウコピーから変更があったブロックレベルのコピーを作成することで機能します。ファイル全体ではなく変更部分のみがコピーされるため、シャドウコピーのために使用されるディスク容量は、現時点でのファイルサイズと同じとは限りません。

シャドウコピーサービスは圧縮ファイルや暗号化ファイルにも対応しています。また、ファイルに設定されたアクセス許可も保持しますので、ファイルを復元した場合、以前と同じアクセス許可が割り当てられます。しかし、削除したファイルを復元する場合は、そのファイルにはディレクトリの既定のアクセス許可が設定されます。

シャドウコピーのデータは一時的なものと認識してください。

シャドウコピーに確保したディスク容量の最大値に達した場合、もしくは、ボリュームごとに保存できるシャドウコピーの最大数である 64 個に達した場合、最も古いシャドウコピーが削除されます。そのため、シャドウコピーを有効にしても通常のバックアップ作業は必要です。大切なデータについては、オプション指定のバックアップソフトを使ってテープ装置などの記憶媒体にバックアップするようにお願いします。

シャドウコピーは読み取り専用です。編集はできません。

6.2　シャドウコピーの設定

シャドウコピーの設定を行う際、以下を決定する必要がありますので、運用環境やファイルの利用状況などから事前に検討してください。

1. シャドウコピーを有効にするボリューム
2. シャドウコピーのために確保するディスク領域
3. シャドウコピーを保存するボリューム
4. シャドウコピー作成のスケジュール

6.2.1　シャドウコピーを有効にするボリューム

シャドウコピーサービスでは、特定のディレクトリやファイルではなくボリューム全体のコピーが作成されます。シャドウコピーは、サーバ上のユーザーのドキュメント、プレゼンテーション資料、データベースファイルなどのファイルを保持しているボリュームに対して有効にしてください。実行ファイルや電子メールなどのデータベースファイルの以前のバージョンへのアクセスを提供するために使用しないでください。シャドウコピーは、ホームディレクトリ、グループポリシーを使用してリダイレクトされるマイドキュメントフォルダ、およびユーザーがデータを保存する共有フォルダなどを含むボリュームに対して設計されています。システム領域を含むボリューム、仮想メモリのページングファイルや休止ファイルを含むボリュームでは、シャドウコピーを有効にしないでください。

シャドウコピーは NTFS ボリュームのみに対応しています。FAT ボリュームでは動作しません。

ネットワーク共有資源を含むボリュームでは、シャドウコピーを有効にしておいてください。

共有フォルダのシャドウコピーに使用するボリュームを最適化する場合、フォーマット時にクラスタ アロケーション ユニットサイズを 16KB 以上に設定することをお勧めいたします。

6.2.2　シャドウコピーのためのディスク容量

シャドウコピーが有効になっているボリューム上では、シャドウコピーのためのディスク容量を制限することができます。指定できる最小ディスク容量は 100MB で、既定ではコピー対象であるソースボリュームの 10%に設定されています。この値は管理者によって変更することができます。使用量が最大値に達した場合は古いシャドウコピーが削除されますので、ユーザーが頻繁にファイル更新を行う場合はこの値を増やす必要があります。

管理者は、ユーザーがどれくらい古いバージョンまでのシャドウコピーを必要としているかを考慮し、シャドウコピーのために確保するディスク容量を十分に検討する必要があります。ユーザーがたった 1 つだけのシャドウコピーしか必要としない場合も、3 日前または 3 週間前までのシャドウコピーを必要とする場合もあります。多くのバージョンのシャドウコピーが必要であれば、より多くのディスク領域を確保する必要があります。

管理者は、シャドウコピーのためのディスク領域を設定する際、サーバに保存されているデータ量ではなく、データがどれくらい更新されるかを検討してください。

シャドウコピーのために確保しているディスク容量に関わらず、1 つのボリュームには最大 64 個のシャドウコピーしか作成できません。65 個目のシャドウコピーが作成されると、一番古いシャドウコピーが削除されます。

6.2.3　シャドウコピーを保存するボリューム

シャドウコピーを保存するボリュームは、既定ではソースボリューム(コピー対象のユーザーデータが保存されているボリューム) と同じですが、同じサーバ上の別のボリュームに変更することができます。たとえば、ユーザーデータが F:¥ に保存されている場合、G:¥ などシャドウコピー保存のための専用のボリュームにシャドウコピーを保存するというような運用が可能です。

シャドウコピーを保存するボリュームを別のディスク上のボリュームに変更するとパフォーマンスが向上します。使用量の多いファイルサーバの場合は、このような運用をお勧めいたします。

ただし、WebUI 画面上でこの設定変更はできませんので、シャドウコピーの保存先を変更したい場合は、リモートデスクトップにて iStorage NS にログオンして操作を行ってください。操作手順に関しては、後に説明いたします。

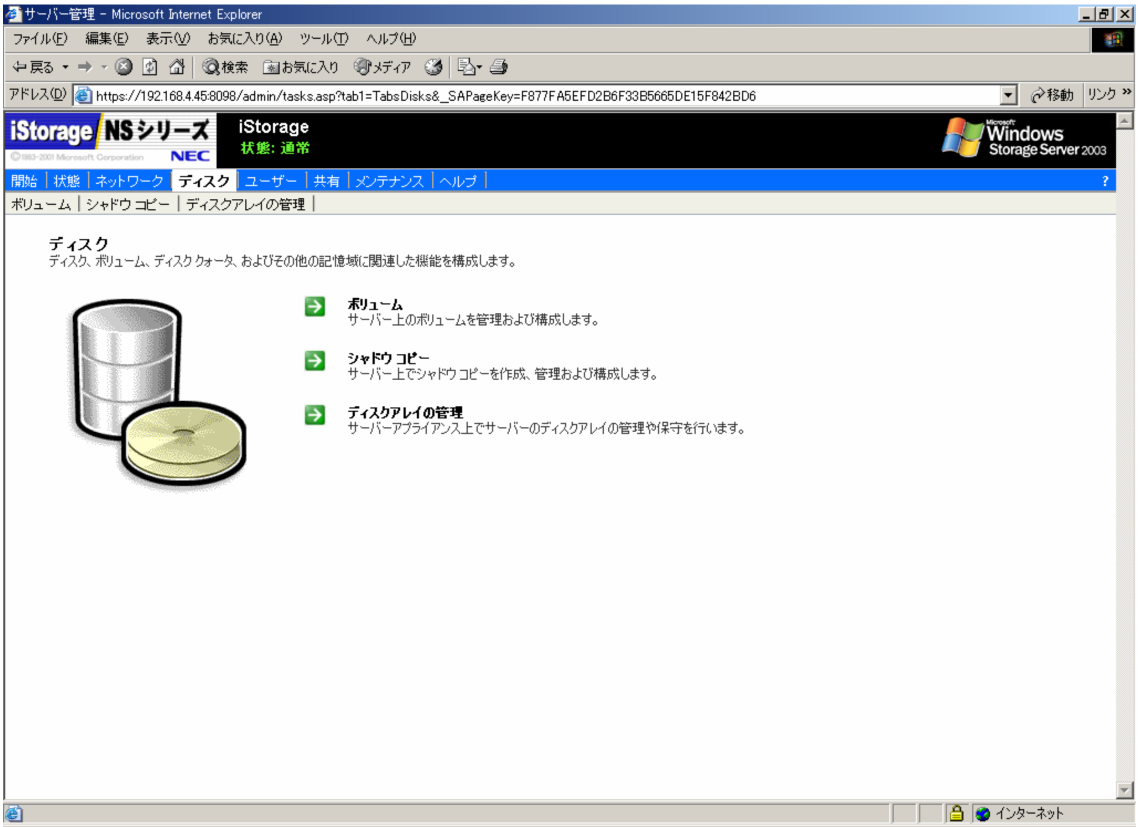
6.2.4　シャドウコピー作成のスケジュール

シャドウコピーはスケジューリング機能を持っています。シャドウコピーを有効にすると、既定で平日の午前 7 時と 12 時にシャドウコピーを作成するスケジュールが設定されます。これらのスケジュールは変更できますので、ご使用の環境や利用方法などに基づいて、シャドウコピー作成のスケジュールを設定してください。シャドウコピーを頻繁に作成すると、ユーザーが必要とするバージョンのシャドウコピーを復元できる可能性が高くなります。しかし、シャドウコピーは 1 つのボリュームにつき最大 64 個しか作成できませんので、シャドウコピー作成の間隔を短くすると早い段階でシャドウコピーが削除される可能性があります。また、作成されるシャドウコピー数が多いほどシャドウコピーによって消費されるディスク領域が増えます。

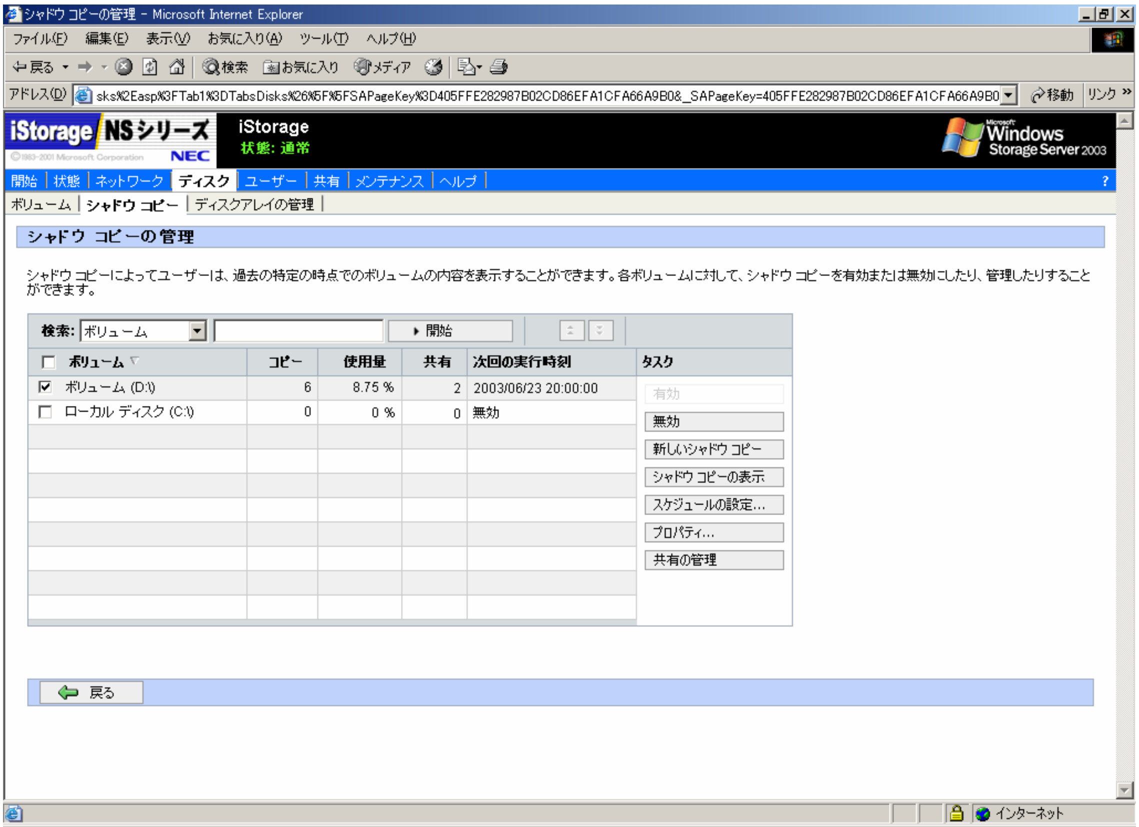
シャドウコピーを作成する頻度は、1 時間につき 1 回までにしてください。

6.3　操作の説明

WebUI の管理画面に接続し[ディスク]を選択すると、以下の画面が表示されます。



上記画面にて[シャドウコピー]を選択すると、次のシャドウコピーの管理画面が表示されます。



[シャドウコピーの管理] ページでは、シャドウコピーサービスを使用してさまざまなタスクを実行できます。対象のボリューム名の横のチェックボックスをチェックし、各タスクをクリックしてください。それぞれのタスクについては後に説明します。

また、このページには以下の情報が表示されます。

- **ボリューム**

  シャドウコピーサービスを使用できるサーバ上のボリュームがすべて表示されます。シャドウコピーは、物理的にサーバ上に存在する NTFS ファイルシステムのデータボリュームのみで使用できます。FATファイルシステムには対応していません。ボリュームのシャドウコピーを管理するには、ボリューム名の横のチェックボックスをチェックして、[タスク] ボックスの一覧から実行するタスクを選択します。

- **コピー**

  ボリュームのシャドウコピーの数が表示されます。

- **使用量**
  ボリュームのシャドウコピーで使用されている合計ディスク領域の使用率が表示されます。

- **共有**
  ボリューム上に存在する共有フォルダの数が表示されます。この情報は、ボリュームのシャドウコピーを有効にするかどうかを判断するときに役立ちます。ボリュームの共有フォルダ数が多いほど、ユーザーがシャドウコピーにアクセスする必要性が高くなります。

- **次回の実行時刻**
  ボリュームのシャドウコピーサービスが有効な場合、次にシャドウコピーを作成する日時がこの列に表示されます。それ以外の場合は、[無効] と表示されます。

〈シャドウコピーを有効にする前に〉

新たにボリュームを追加する場合、シャドウコピーを有効にするボリュームは、16KB 以上のアロケーション ユニット サイズでフォーマットすることをお勧めします。16 KB 以上に設定しないと、最適化の結果、シャドウコピーが削除されることがあります。

また、システム領域を含むボリューム、および、仮想メモリのページング ファイルや休止ファイルを含むボリュームではシャドウコピーを有効にしないでください。

6.3.1　有効／無効

ボリュームのシャドウコピーを有効にすると、いくつかの処理が自動的に実行されます。選択したボリュームのシャドウコピーが作成され、シャドウコピーの最大記憶域が設定されます。さらに、平日の午前 7 時と 12 時にシャドウコピーを作成するスケジュールが設定されます。単にシャドウコピーを作成した場合は、ボリュームのコピーが 1 つ作成されるだけでスケジュールは設定されません。

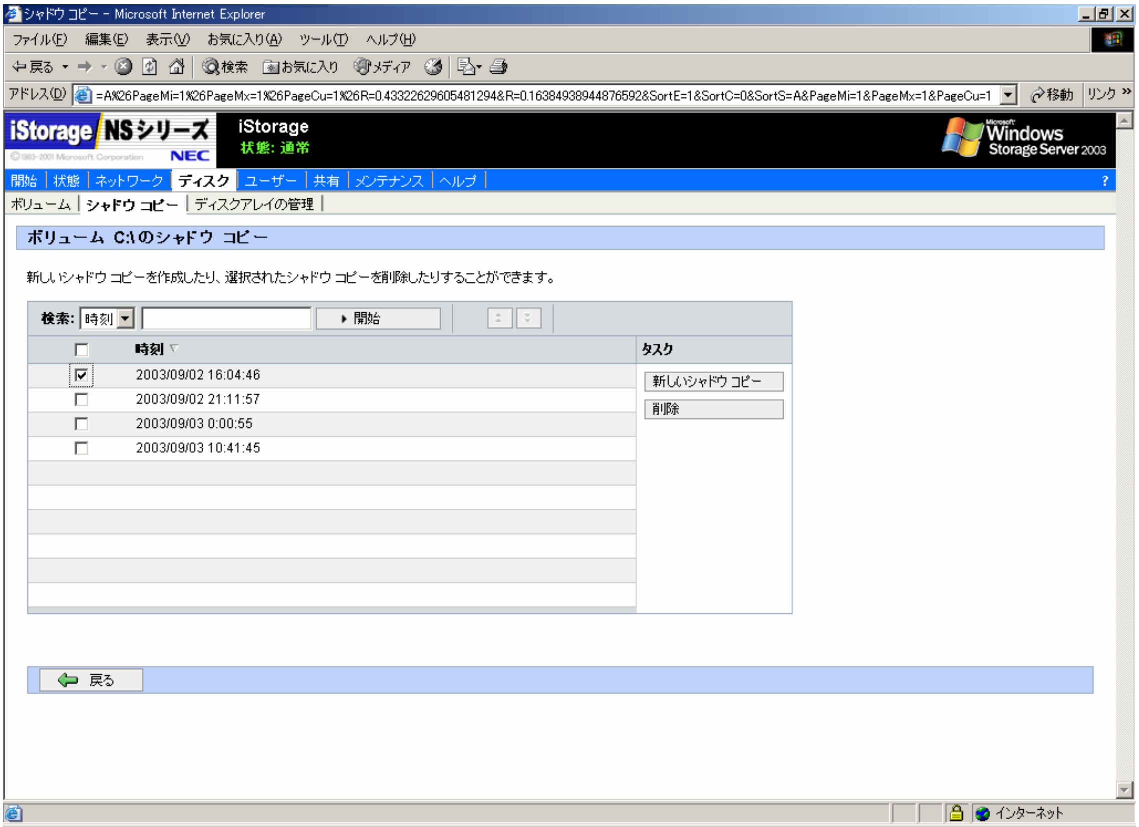
ボリュームのシャドウコピーを無効にすると、そのボリューム上に存在するすべてのシャドウコピー、およびシャドウコピーのスケジュールが削除されます。

6.3.2　新しいシャドウコピー

シャドウコピーの作成は、スケジューリングによる作成と手動での作成の 2 つの方法があります。手動でシャドウコピーを作成する場合は、シャドウコピーを作成したいボリュームのチェックボックスをチェックし、タスクの[新しいシャドウコピー]をクリックしてください。複数のボリュームを選択し、同時にシャドウコピーを作成することも可能です。スケジューリングによる作成については後に説明いたします。

6.3.3　シャドウコピーの表示

作成されているシャドウコピーを表示する場合は、対象ボリュームのチェックボックスをチェックし、[シャドウコピーの表示]をクリックしてください。以下のような画面が表示され、現在、保存されているシャドウコピーが表示されます。



シャドウコピーのタスクとして、[新しいシャドウコピー]、[削除]があります。

1）新しいシャドウコピー

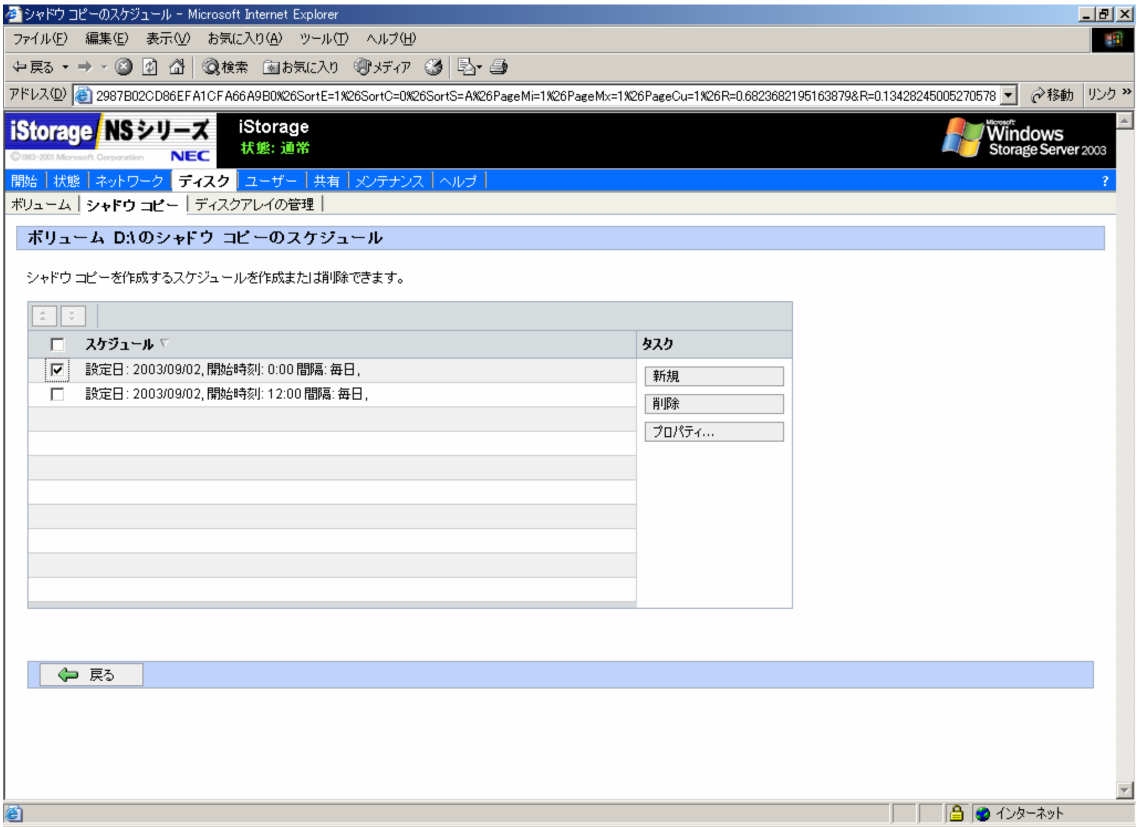
選択したボリュームのシャドウコピーを手動で作成します。タスクの[新しいシャドウコピー]をクリックすることで、シャドウコピーが作成されます。

2）削除

シャドウコピーの削除を行います。保存されているシャドウコピーの一覧が表示されていますので、削除したいシャドウコピーのチェックボックスをチェックし、[削除]をクリックしてください。削除するかどうかの確認のページが表示されます。そこで[OK]をクリックすればシャドウコピーが削除されます。

6.3.4　　スケジュールの設定

シャドウコピーを作成するスケジュールを指定します。



スケジュールのタスクとして[新規]、[削除]、[プロパティ]があります。

1）新規

新規にスケジュールを設定します。新規にスケジュールを作成する場合はタスクの[新規]をクリックしてください。シャドウコピーの作成頻度(1 回のみ／毎日／毎週／毎月)、スケジュールをスタートさせる日時を指定してください。設定が終わりましたら[OK]をクリックしてください。スケジュールが登録されます。

2）削除

スケジュールの削除を行います。現在登録されているスケジュールが一覧として表示されています。削除したいスケジュールのチェックボックスをチェックし、[削除]をクリックしてください。削除するかどうかの確認のページが表示されます。そこで[OK]をクリックすればスケジュールが削除されます。

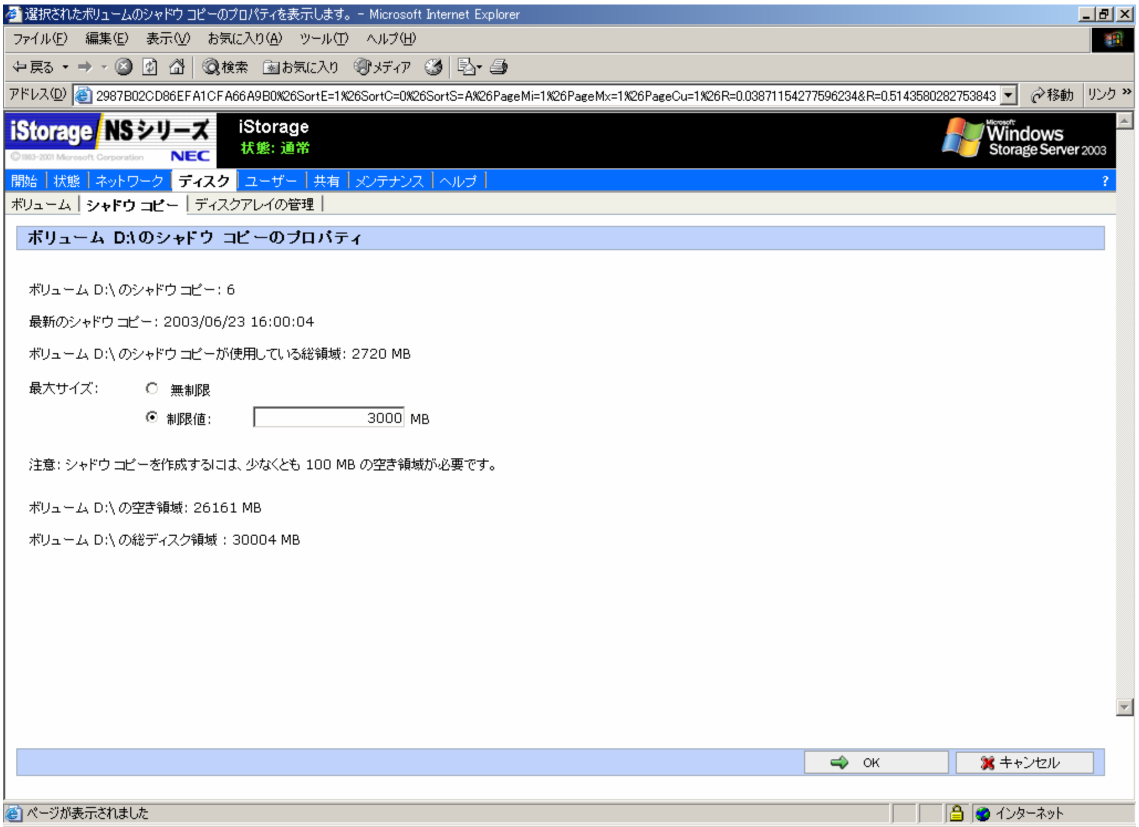
3）プロパティ

スケジュールの設定の参照、変更を行います。現在登録されているスケジュールが一覧として表示されています。参照したいスケジュールのチェックボックスをチェックし、[プロパティ]をクリックしてください。指定のスケジュール情報の参照および変更ができます。

シャドウコピーの作成頻度は、1 時間につき 1 回までにしてください。

6.3.5 プロパティ

ボリュームのシャドウコピーの設定およびシャドウコピーの数に関する情報が表示されます。このページを使用して、シャドウコピーが使用できる最大ディスク容量を設定することができます。



シャドウコピーが使用できる最大ディスク容量の既定値は、ソースボリュームのサイズの 10%です。この値は変更可能ですが、この値を大きくしても 1 つのボリュームに作成できるシャドウコピーは最大 64 個です。

シャドウコピーのサイズ制限を小さくするときは注意が必要です。現在、シャドウコピーで使用している合計サイズより小さいサイズを設定すると、新しいサイズ制限に合わせて古いシャドウコピーが削除されます。削除されたシャドウコピーは元に戻すことができません。

6.3.6　シャドウコピーの保存先の変更

シャドウコピーの保存先をソースボリューム(コピー対象のユーザーデータが保存されているボリューム)とは別のボリュームに変更したい場合は、リモートデスクトップにて iStorage NS にログオンして以下の操作を行ってください。WebUI 画面上ではこの操作を行うことができません。また、この設定変更を行う前に、すべてのシャドウコピーを削除する必要があります。

1. リモートデスクトップにて iStorage NS にログオンしてください。
   リモートデスクトップについては、「2.1.3 リモートデスクトップ(ターミナルサービス) について」を参照してください。
2. [コンピュータの管理] を開きます。
3. コンソールツリーで [共有フォルダ] を右クリックし、[すべてのタスク] を選択して、[シャドウ コピーの構成] をクリックします。
4. 変更するボリュームをクリックし、[設定] をクリックします。
5. [設定] ダイアログ ボックスで、必要に応じて設定を変更します。

6.4 シャドウコピークライアントのセットアップ

シャドウコピーを利用してファイルやディレクトリの復元を行う場合、クライアントコンピュータから復元操作を行います。クライアントコンピュータとして動作するのは、Windows Server 2003、Windows XP、Windows 2000 (SP3 以降) および UNIX クライアント のみです。Windows NT 4.0、Windows Me, Windows 9x には対応しておりません。Windows Server 2003、UNIX クライアント の場合は、標準で復元操作が可能ですが、Windows XP(*1)、Windows 2000 に関しては、シャドウコピーにアクセスするためのシャドウコピークライアントのインストールが必要となります。インストール方法に関しては次に説明いたします。

(*1) Windows XP SP2 を適用するとシャドウコピークライアントが自動的にインストールされます。

6.4.1 クライアントのセットアップ手順

Windows XP、Windows 2000 クライアントの場合は、マイクロソフトのホームページから、シャドウコピークライアント セットアップモジュールをダウンロードし、セットアップを行ってください。Windows Server 2003、UNIX クライアントの場合は、クライアントモジュールのセットアップ操作は必要ありません。

http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=e382358f-33c3-4de7-acd8-a33ac92d295e

(2006 年 3 月 29 日現在)

1. クライアントコンピュータで[ダウンロード]リンクをクリックして、ダウンロードを開始してください。

2. すぐにインストールを行う場合は、[開く]をクリックしてください。後でインストールを行う場合は、[保存] をクリックしてください。

クライアントモジュールをインストールすることで、ネットワーク共有上のファイルおよびフォルダの[プロパティ]ダイアログボックスに[以前のバージョン]タブが追加されます。ユーザーは、[以前のバージョン]タブにある[表示]、[コピー]、[復元]の 3 つのオプションをそれぞれ選択することができます。

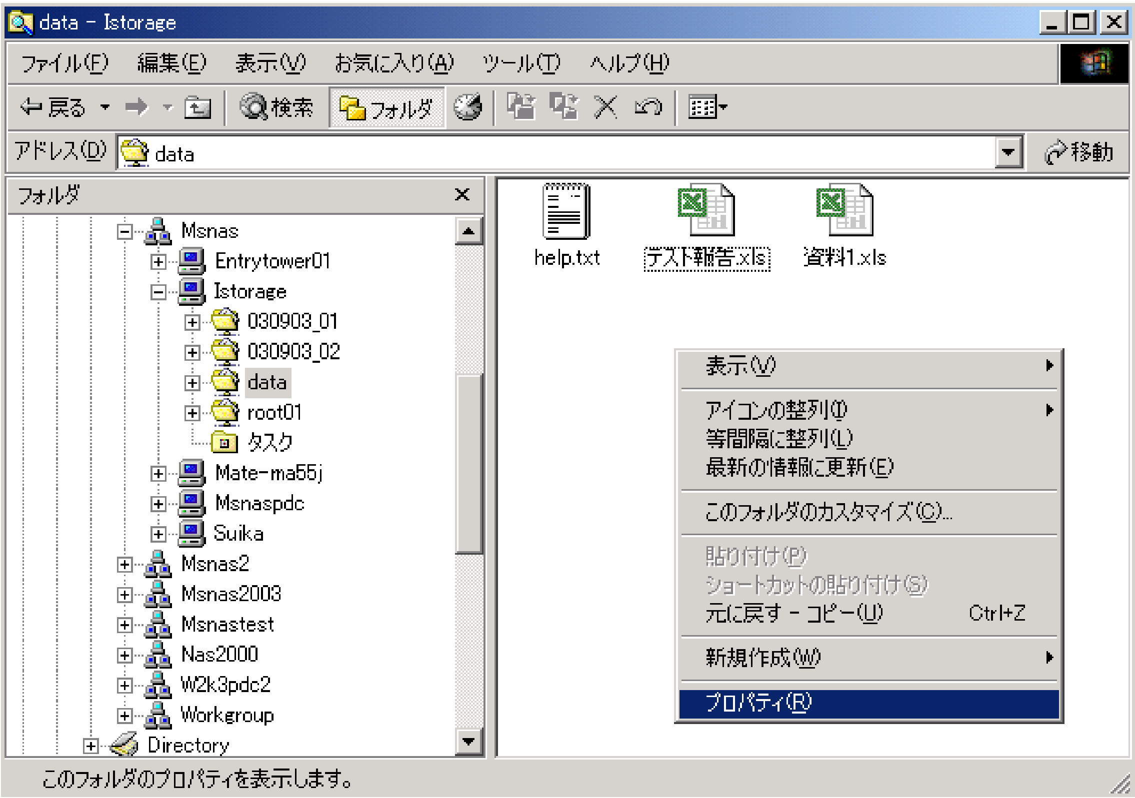
6.5 Windows クライアントからの復元操作

シャドウコピーサービスを利用してファイルやディレクトリの復元操作を行う場合は、クライアントコンピュータ上のエクスプローラから操作を行ってください。

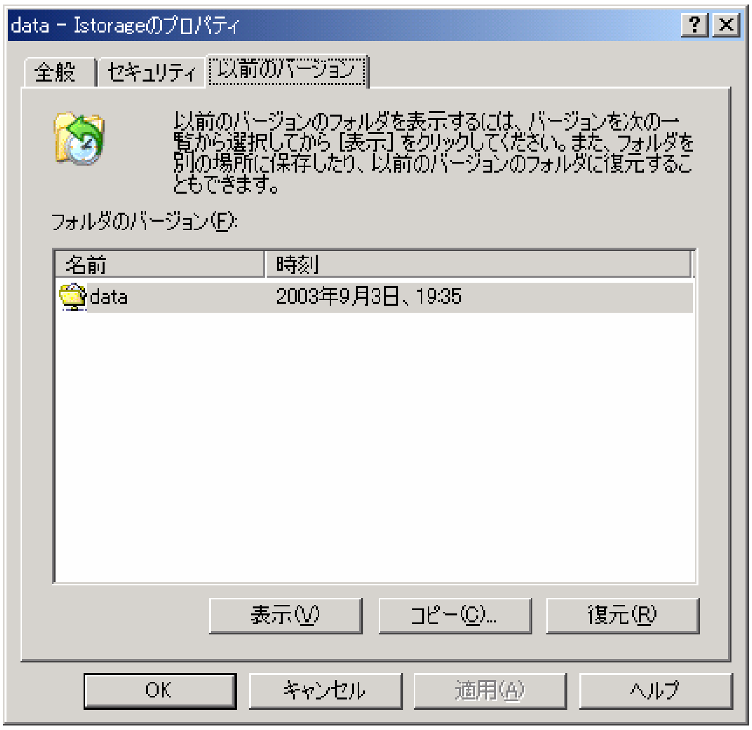
6.5.1 削除したファイルの復元

削除したファイルを復元する場合は、以下の手順に従って、クライアント上のエクスプローラから操作を行ってください。

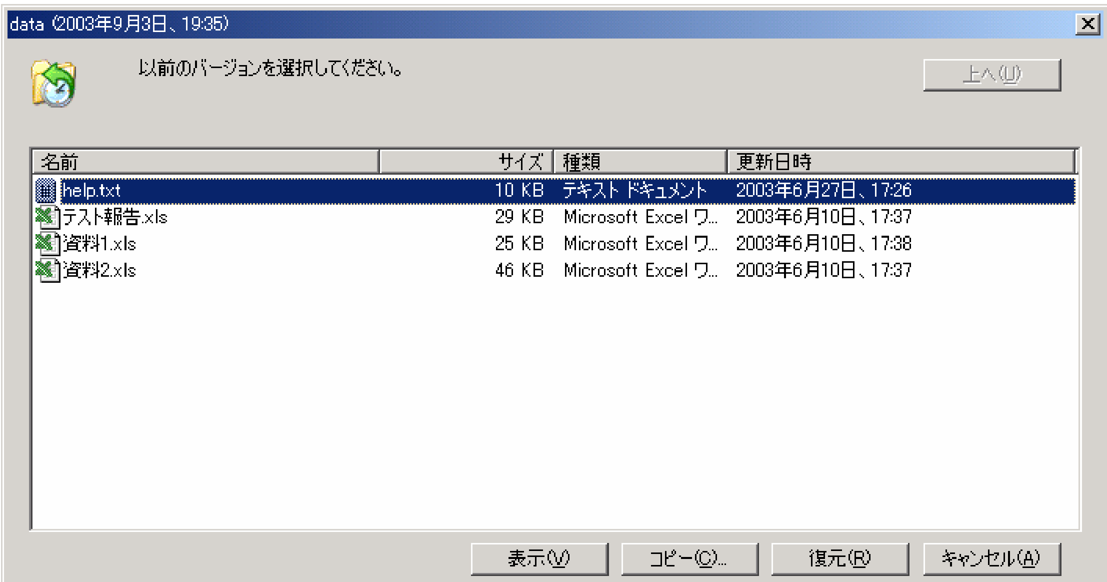
1. 削除したファイルが格納されていたフォルダを選択してください。
2. 選択したフォルダ内で右クリックし、[プロパティ]メニューをクリックしてください。



3. プロパティ画面にて[以前のバージョン]タブをクリックしてください。



4. 削除される前のファイルを含むフォルダのバージョンを選択し、[表示]をクリックしてください。
5. シャドウコピー作成時のフォルダ配下のファイルが表示されるので、復元したいファイルを選択してください。

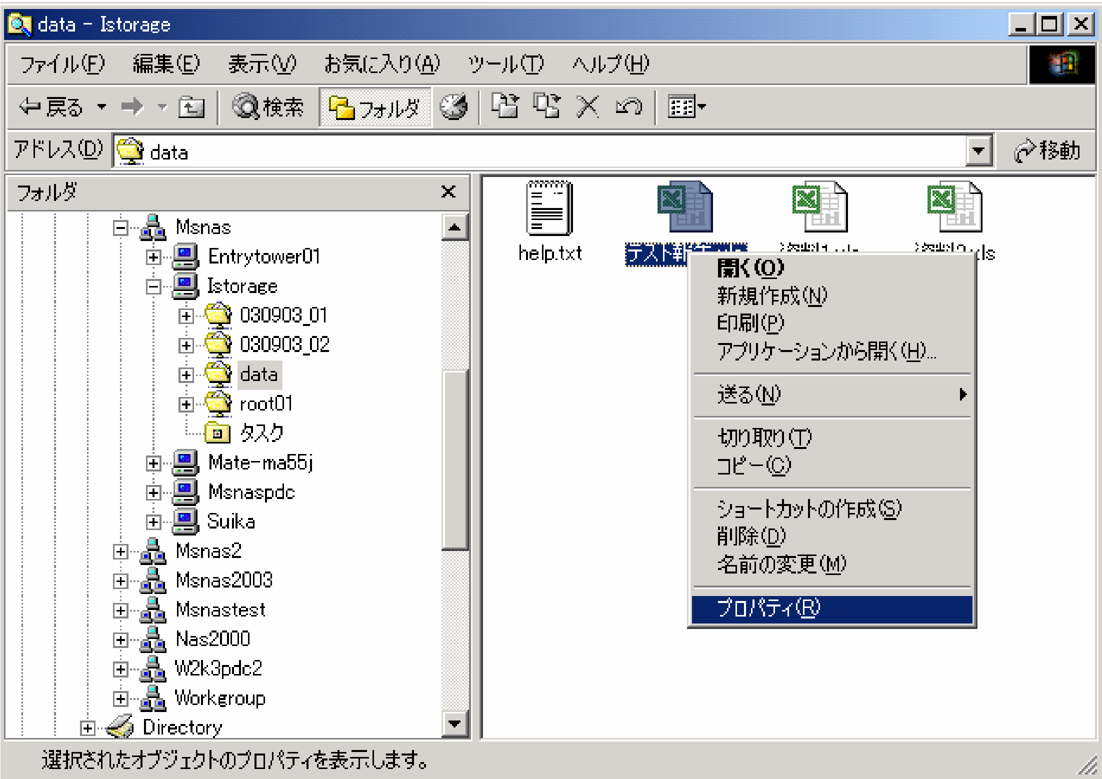


6. 他の場所にコピーしたい場合は、[コピー]をクリックしてください。また、復元したいのであれば[復元]をクリックしてください。

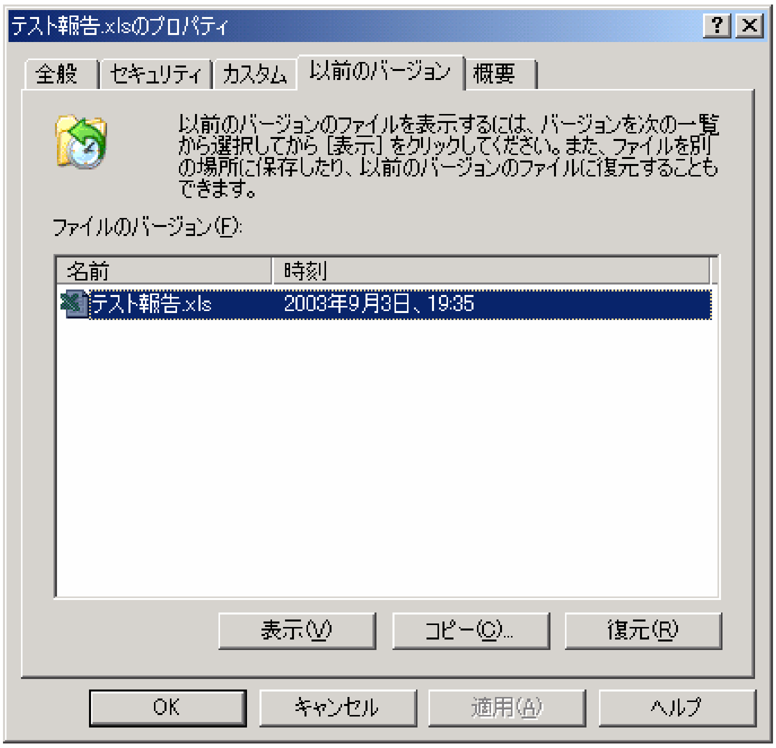
6.5.2 更新したファイルの復元

誤って更新したファイルや壊れたファイルを復元する場合は、以下の手順に従って、クライアント上のエクスプローラから操作を行ってください。この場合、復元したいファイル自体を右クリックすることができるため、削除したファイルを復元する場合よりも簡単に復元操作を行うことができます。

1. 誤って更新したファイル(もしくは壊れたファイル)を選択してください。
2. 選択したファイルを右クリックし、[プロパティ]メニューをクリックしてください。



3. プロパティ画面にて[以前のバージョン]タブをクリックしてください。

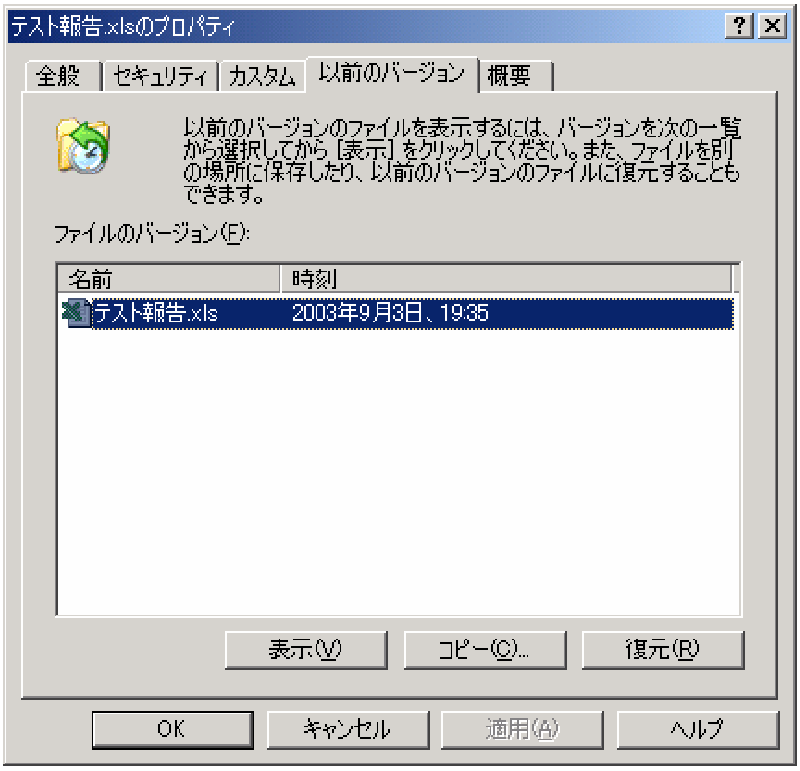


4. 古いバージョンのファイルを参照したいのであれば、[表示]をクリックしてください。他の場所にコピーしたい場合は[コピー]をクリックしてください。また、復元したいのであれば[復元]をクリックしてください。

6.5.3　フォルダの復元

フォルダを復元したい場合は、以下の手順に従って、クライアント上のエクスプローラから操作を行ってください。

1. 復元したいフォルダを選択してください。
2. 右クリックにて[プロパティ]をクリックし、プロパティ画面にて[以前のバージョン]タブをクリックしてください。



3. [コピー]もしくは[復元]をクリックしてください。
   [復元]を選択すると、そのフォルダだけでなくサブフォルダまですべて復元されます。

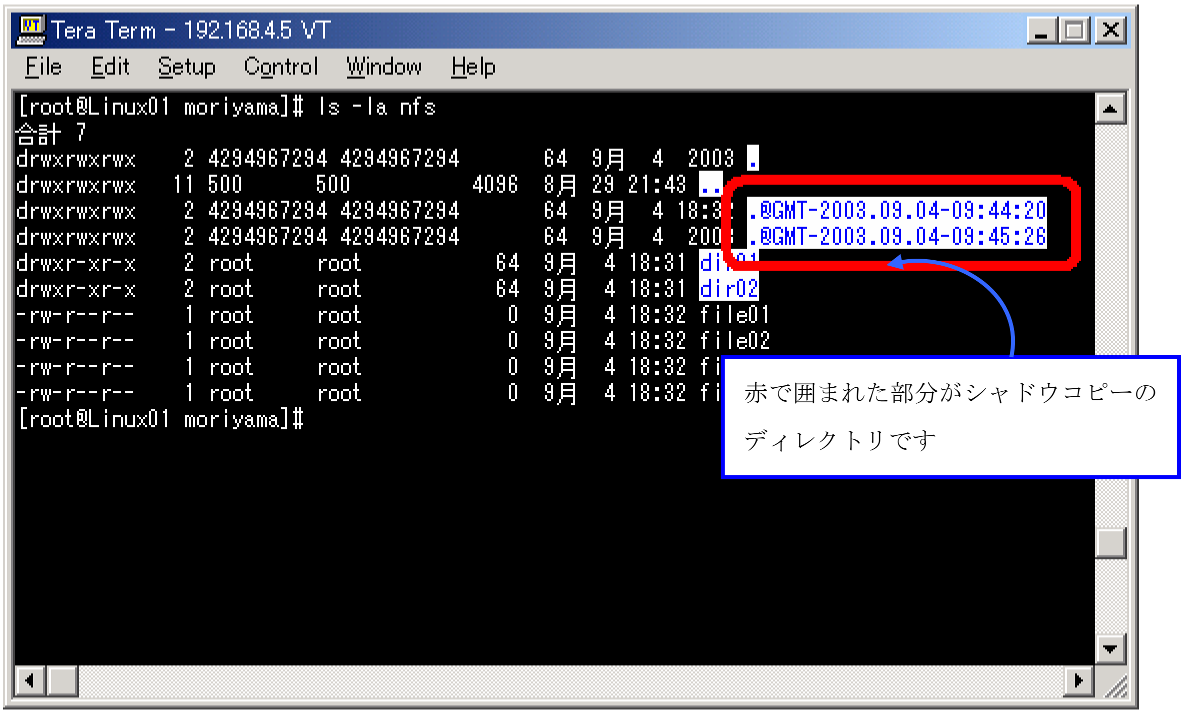
> [復元]操作を実施しても、シャドウコピー作成後に作成されたファイルが削除されることはありません。

6.6 UNIXクライアントからの復元操作

UNIX クライアントからもシャドウコピーでバックアップしたファイル、ディレクトリを復元することが可能です。

バックアップされたファイル、ディレクトリは NFS 共有直下に、".@GMT-(日付)"というディレクトリとして表示されます。UNIX クライアントから復元操作を行う場合は、該当する日時のシャドウコピーのディレクトリ配下より復元したいフォルダまたはファイルをコピーして下さい。

ディレクトリ名に設定されている日時はグリニッジ標準時にて設定されています。



シャドウコピーは読み取り専用です。編集はできません。

6.7 シャドウコピーサービスに関する注意事項

- シャドウコピーは、NTFS ファイルシステムのデータボリュームのみに対応しています。FAT ファイルシステムには対応していません。
- システム領域を含むボリューム、また、仮想メモリのページングファイルや休止ファイルを含むボリュームでは、シャドウコピーサービスを有効にしないでください。
- シャドウコピーは１つのボリュームにつき最大64個まで作成できます。それ以上シャドウコピーが作成された場合、一番古いシャドウコピーが削除されます。
- シャドウコピーのサイズ制限を小さくするときは注意が必要です。現在、シャドウコピーで使用している合計サイズより小さいサイズを設定すると、新しいサイズ制限に合わせて古いシャドウコピーが削除されます。削除されたシャドウコピーは元に戻すことができません。
- シャドウコピーを有効にするボリュームで最適化を実行する予定がある場合は、そのボリュームを 16 KB 以上のアロケーションユニットサイズでフォーマットすることをお勧めします。この方法をとらないと、ボリュームを最適化した結果、シャドウコピーが削除されることがあります。
- シャドウコピーの作成頻度は、1時間に1回までにしてください。
- シャドウコピー作成のスケジュールは、できるだけバックアップツール等との動作時刻と重ならないような時間帯を設定してください。
- 管理者は、ユーザーに対して、シャドウコピーがどれくらいの頻度で作成されるのかを通知しておいてください。また、作成できるシャドウコピー数は64個までであり、その後は最も古いコピーが削除されることも通知する必要があります。
- サーバにて高負荷の入出力処理が発生した場合、シャドウコピーが全て削除されるという現象があります。詳細および回避策については次に記載いたします。

6.7.1 高負荷状態でシャドウコピーが削除される現象について

シャドウコピーを有効にし、そのボリュームでファイル更新等を行うと差分情報をシャドウコピーの記憶域に書き込みますが、記憶域が不足すると記憶域を必要に応じて制限値まで拡張させます。しかし、高負荷の入出力処理が続き、そのシャドウコピー記憶域の拡張が間に合わなくなった場合、シャドウコピーの仕様により保存しているシャドウコピーが全て削除されます。

iStorage NS シリーズでは、シャドウコピーの記憶域の初期値をあらかじめ大きくすることで、この現象をできるだけ回避するようにしております。そのため、WebUI のシャドウコピーのプロパティ画面上には 「シャドウコピーを作成するには、少なくとも 100MB の空き領域が必要です。」と表示されていますが、iStorage NS シリーズでは 300MB の空き容量が必要となっております。

(**iStorage NS430/NS510G/NS130/NS43P/NS23P** を除く)

上記のように iStorage NS シリーズでは、シャドウコピーの記憶域の初期値を 300MB に変更していますが、それでも不十分でシャドウコピーが全て削除されてしまう場合は、シャドウコピーの記憶域の初期値を変更してください。ディスクに余裕がある場合は、この値をさらに大きく設定することをお勧めいたします。最大 3GB まで設定可能です。シャドウコピーの記憶域の初期値を変更する場合は、次の手順に従って操作を行ってください。

< 事前確認 >

シャドウコピーの記憶域の初期値を設定する前に、以下を確認してください。

1. シャドウコピーの記憶域のボリュームに、設定したい初期値分の空きがあること。
2. シャドウコピーの記憶域の最大値が、設定したい初期値より大きく設定していること。

< 初期値の変更手順 >

以下の手順に従って、レジストリの値を変更してください。

1. WebUI の[メンテナンス]-[リモートデスクトップ]をクリックし、管理者権限のアカウントを使用してログオンします。
2. レジストリエディタを起動し、次のレジストリキーを選択します。
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥VolSnap
3. [編集]メニューの[新規]を選択し、[DWORD 値]をクリックします。
4. **MinDiffAreaFileSize** と入力し、Enter キーを押します。
5. [編集]メニューの[修正]をクリックします。
6. 設定するシャドウコピーの記憶域の初期値を入力し、[OK]をクリックします。
7. レジストリエディタを終了します。
8. リモートデスクトップをログオフします。

このレジストリ値 **MinDiffAreaFileSize** には、シャドウコピーの記憶域の最小サイズを指定します。規定値は 300MB、設定可能な最大値は 3GB です。(レジストリに 300 を指定すると 300MB、3000 を指定すると 3GB です。) なお、設定は 300MB の倍数を設定してください。300MB の倍数でない値を設定すると、次に大きい 300MB の倍数の値が使用されます。

(注) この値には、シャドウコピーの記憶域の最大サイズを超える値を設定しないでください。シャドウコピーが正常に機能しない場合があります。

レジストリエディタの使い方を誤ると、深刻な問題が発生する可能性があります。最悪の場合、システムの再インストールが必要になることがありますので、十分ご注意の上、操作を行ってください。

アップデートモジュールについて

PP・サポートサービスにご加入されている **iStorage NS430/NS510G/NS130/NS43P/NS23P** をお使いのお客様には、シャドウコピー記憶域の初期サイズを拡張するアップデートモジュールを、以下のタイトルにて PP・サポートのホームページで公開しております。必要に応じてアップデートモジュールを適用してください。

タイトル：「iStorage NS シリーズ シャドウコピー記憶域 初期サイズ拡張のための
アップデートモジュール」

7 Windows(SMB) アクセス

Windows SMB (Microsoft Server Message Block)は、Windows 環境でのファイル共有プロトコルです。Windows2003 で使用されている SMB のバージョンには（CIFS）も含まれます。

7.1 Windows（SMB）共有

iStorage NS 内に新たに Windows 共有を作成するには、以下の手順で行います。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します。
2. WebUI の[共有]→[共有]をクリックします
3. タスクの[新規]をクリックします
4. 共有名、共有パスなどを設定し、Windows (Microsoft SMB)にチェックします。
5. [Windows 共有]タブをクリックします
6. アクセス権などの設定を行った後、[OK]ボタンをクリックします。

7.2 Windows(SMB)クライアントからのアクセス

WindowsXP/NT/2000/2003 マシンをクライアントとして iStorage NS 上の SMB（CIFS）による共有へアクセスするには、管理 PC の「マイネットワーク」から、iStorage NS が属するドメインまたはワークグループ内にある iStorage NS に付けたコンピュータ名のアイコンを開くことで、その iStorage NS が SMB によって提供している共有にアクセスできます。

7.3 Windows(SMB)のアクセス制御

ユーザーや複数のユーザーをまとめたグループに対して各共有へのアクセスを制限する事で、セキュリティを保ったファイルアクセスの管理を行います。アクセス制御によって、必要なユーザーだけにファイルをアクセス可能にし、不必要なユーザーからのアクセスを禁止することで、不正な参照や書き換え、削除を防止します。

Windows（SMB）による共有内のフォルダ・ファイルへのアクセス制御は大きく２つに分けられます。1 つは共有レベルのアクセス制御、もう１つはファイルシステムレベルのアクセス制御です。共有レベルのアクセス制御は、共有を作成する際に指定します。（作成後に[プロパティ]メニューから変更する事もできます。）共有に設定できるアクセス制御は、以下の特徴を持ちます。

- ユーザー／グループ単位で設定できます。
- 各ユーザー／グループには、[フルコントロール]、[読み取り]、[変更／読み取り]、アクセス権[なし]を指定できます。
- 許可する権限だけでなく、拒否する権限という形でも指定できます。

> アクセス権の設定は必ず行ってください。デフォルトでは everyone に「読み取り」のアクセス権が設定されています。

Windows(SMB)アクセス

Windows（SMB）による共有のアクセス権は以下の手順で設定します。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します
2. WebUI の[共有]→[共有]をクリックします
3. アクセス権の設定を行う共有名にチェックし、[プロパティ]を選択します
4. [Windows 共有]タブを選択します
5. 各ユーザーにアクセス権を設定します

ドメインユーザー／グループへのアクセス権を設定する場合は、上図の「ユーザーまたはグループの追加」の下の入力フィールドに「*ドメイン名¥ユーザー名*」または「*ドメイン名¥グループ名*」の形式で入力し、[追加]ボタンをクリックして、許可、拒否の設定を行ってください。設定を反映させるには、 [OK]ボタンをクリックしてください。

ファイルシステムレベルのアクセス制御は、リモートデスクトップを起動して設定を行ないます。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します
2. WebUI の[メンテナンス]→[リモートデスクトップ]を選択してリモートデスクトップを起動します
3. 管理者権限のアカウントとパスワードでログオンします
4. マイコンピュータまたはエクスプローラで共有設定したフォルダまたはファイルを右クリックし、プロパティを選択します
5. [セキュリティ]タブをクリックします
6. 以下、Windows での NTFS のアクセス権の設定と同じです。（同様に「監査」の設定や「所有権」の取得も可能です。）

共有レベルのアクセス権で、共有に対するユーザーのアクセスを制御し、更に共有内のフォルダやファイルに対してファイルシステムレベルのアクセス制御を設定する事で、細かなアクセス制御を行う事が可能です。（例えば、共有レベルであるユーザーにフルコントロールを与えても、その共有内のあるフォルダ配下はアクセスに禁止するなどの設定が可能です。）

8 NFSアクセス

iStorage NS14PW にて NFS を利用する場合、512MB 以上のメモリを搭載してください。
また、出荷時はサービスが無効になっていますので、後述の手順に従ってサービスを開始させてください。

NFSアクセス

出荷時、NFS が無効となっている機種(**NS14PW**)において、NFS をご利用になる場合は、以下の手順に従って、サービスを開始させてください。

1. WebUI の[メンテナンス]→[リモートデスクトップ] をクリックし、管理者権限のアカウントを使用してログオンします。
2. [管理者メニュー] より、[サービス] を起動します。
3. [Server for NFS] サービスのプロパティにて、スタートアップの種類を[自動]にして、[開始]ボタンをクリックします。
4. [User Name Mapping] サービスのプロパティにて、スタートアップの種類を[自動]にして、[開始]ボタンをクリックします。
5. [OK]ボタンをクリックして、プロパティ画面を閉じます。

8.1 ユーザー／グループ名のマッピング

iStorage NS では、ファイルサービスのプロトコルとして NFS をサポートしています。NFS は UNIX クライアントからファイルアクセスを行うためのプロトコルです。NFS により、UNIX クライアントから iStorage NS 上のファイルを利用可能になります。ただし、UNIX ユーザーが iStorage NS 上のファイルを利用するためには、UNIX ユーザー／グループを Windows ユーザ／グループに変換する必要があります。このことをマッピングと言います。

ユーザー／グループのマッピングでは、UNIX／Windows のユーザー／グループの管理方法によって、それぞれ以下のいずれかを組み合わせることができます。

- UNIX側
  - NIS サーバで管理
  - スタンドアロンの UNIX 装置で管理（パスワードファイル／グループファイルを、iStorage NS 上にコピーする必要があります）
- Windows側
  - ドメインで管理
  - iStorage NS で管理

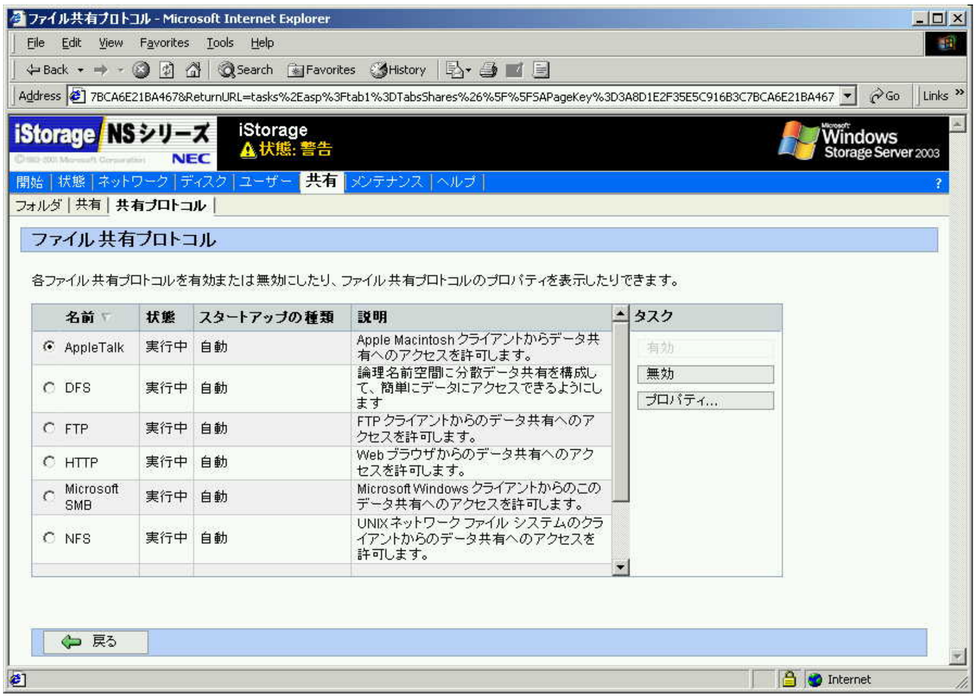
また、マッピング方法として、以下の 2 通りが指定できます。

- 簡略マッピング
  UNIX環境とWindows環境で同一のユーザー名／グループ名を持つユーザー／グループを暗黙的にマッピングします。同一の名前を持たない場合はマッピングされません。
- 明示的なマッピング
  UNIX環境のユーザー／グループとWindows環境のユーザー／グループを手動でマッピングします。

8.1.1 ユーザー／グループマッピングの設定

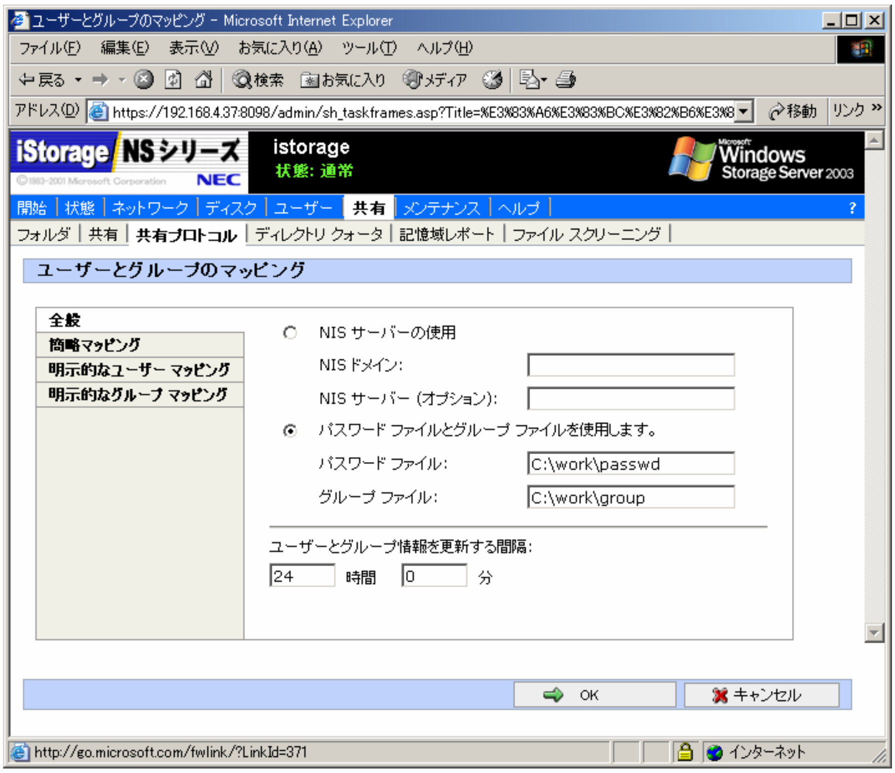
ユーザーマッピングは以下の手順で行います。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します。
2. [共有]→[共有プロトコル]をクリックします。
3. **名前の欄の**[NFS]を選択し、[プロパティ]をクリックします。



図．ファイル共有プロトコル選択

4. [ユーザーとグループのマッピング]をクリックします。
5. NIS サーバを使用している場合は、[NIS サーバ使用]をチェックし、NIS ドメイン名を入力します。NIS サーバを使用していない場合は、[パスワードファイルとグループファイルを使用します]をチェックし、パスワードファイル、グループファイルの格納場所を入力します。パスワードファイルとグループファイルは、事前に UNIX 装置から iStorage NS 上にコピーしておきます。

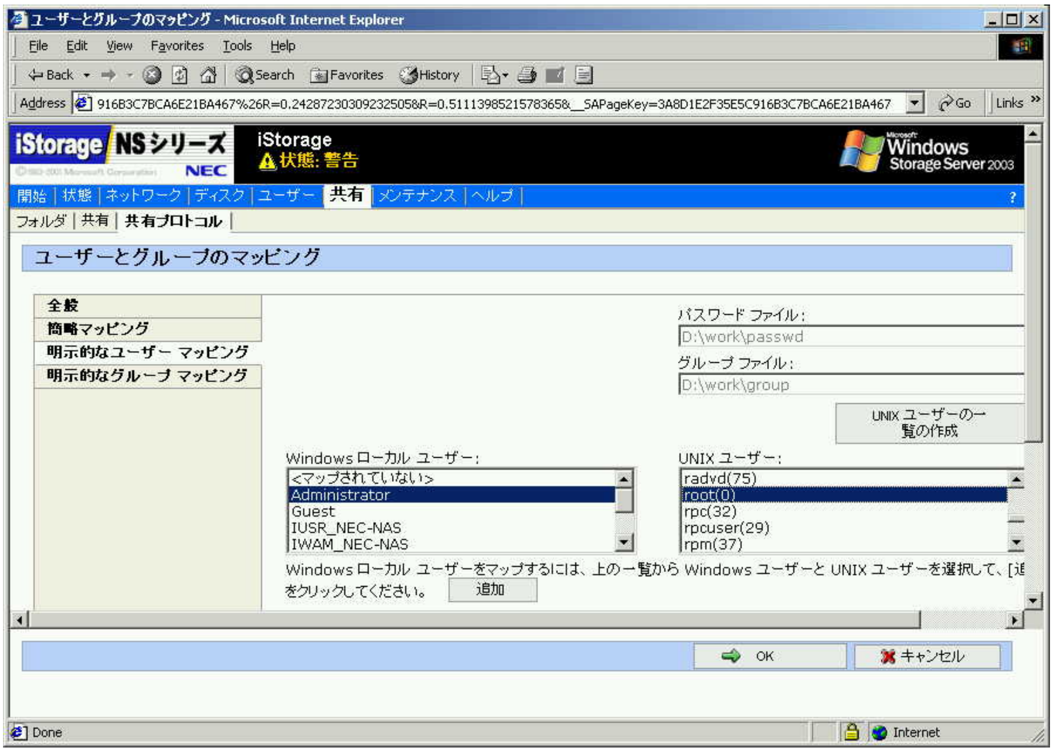


図．ユーザーマッピング

NIS サーバを指定している場合、[NIS ユーザとグループ情報を更新する間隔]を短く設定するとユーザの登録数が多い場合などに、iStorage NS が高負荷状態に陥ることがあります。[NIS ユーザとグループ情報を更新する間隔]の設定値はデフォルト値以上を設定することをお勧めいたします。

以降、簡略マッピングを行う場合は 6.へ、明示的なマッピングを行う場合は 8.へ進みます。

6. [簡略マッピング]タブをクリックします。
7. [簡略マッピングを有効にする]にチェックを付け、ドメイン又はコンピュータ名を指定して [OK]を押して設定を完了します。
8. [明示的なユーザーマッピング]タブを選択します。
9. Windows, UNIX のユーザー,のリストを表示させ、マップするユーザーの組を選択して[追加]します。
10. 全てのユーザーマッピングを行ったら[OK]ボタンをクリックします。
11. 次に、[明示的なグループマッピング]タブを選択します。
12. Windows, UNIX のグループのリストを表示させ、マップするグループの組を選択して[追加]します。



図．ユーザーとグループのマッピング

13. 全てのグループマッピングを行ったら[OK]ボタンをクリックします。

また、明示的にユーザー／グループマッピングする場合は、コマンドラインで行うこともできます。
この場合、以下のように mapadmin add コマンドを使用します。詳細は、mapadmin /? を実行して表示されるヘルプを参照してください。

mapadmin add -wu <Windows ユーザー> -uu <UNIX ユーザー>
（mapadmin add -wg <Windows グループ> -ug <UNIX グループ>）

UNIX情報の取得にpasswd、groupファイルを指定している場合にこのコマンドを使用する場合は、ユーザー名/グループ名の前にPCNFSを付加するようにしてください。

例)windows グループ[users]と UNIX グループ[other]を明示的マッピングする場合

mapadmin add -wg ¥¥ns600¥users -ug PCNFS¥other

8.1.2　rootのマッピングについて

root（UNIX）のマッピングは、一般ユーザーにおけるマッピング設定以外に、NFS 共有の設定を必要とします。詳しくは 8.4 NFS のアクセス制御を参照してください。

root をスーパーユーザとして使用する場合は、root（Unix）と administrator（Windows）をマッピングしてください。

8.1.3　手動によるマッピングの同期

NFS 共有でのユーザーとグループのマッピングで使用されている UNIX ユーザー、グループ情報は出荷時の設定では 24 時間間隔で更新されますが、手動で更新することも可能です。
通常、iStorage NS再起動時の時刻を基準にユーザーマッピングは行われますが、この手動マッピングを行った場合、その行った時間を基準にして次回のマッピングが行われます。
(例：24時間間隔の設定の場合、手動マッピングの実施後、24時間後に自動マッピングが実施されます。)

1. WebUI の[メンテナンス]→[リモートデスクトップ]をクリックします。
2. 管理者権限のあるアカウントを使用してログオンします。
3. [スタート]→[すべてのプログラム]→[Windows Services for UNIX]→[Services for UNIX Administration]を起動します。
4. 左のツリーより[User Name Mapping]を選択し、[Config]タブを開き[Synchronize Now]ボタンを押下します。
5. [Services for UNIX Administration]を終了し、リモートデスクトップからログオフします。

iStorage NS では、モデルによって SFU のバージョン 3.0 またはバージョン 3.5 をサポートしています。
上記は、SFU3.5 を例に記載しています。SFU3.0 の場合は、以下のように表示されます。

[Windows Services for UNIX] → [Microsoft Services for NFS]
[Services for UNIX Administration] → [Services for NFS Administration]

8.1.4 Windows環境からファイルを作成する場合について

NFS 共有フォルダに NFS 以外の環境(Windows、FTP/HTTP 等)からファイルを作成した場合に、UNIX クライアントからファイルの所有者、グループ、アクセス権が正しく表示されないことがあります。

NFS 共有の仕組みの概要は以下のとおりです。

■ ユーザーマッピングについて
ユーザーマッピングにはWindows上のファイル属性のファイル所有者とファイルグループ（プライマリグループ）が使用されます。
注：ファイルグループはPOSIX用のパラメータであり通常Windowsからは使用されません。

■ アクセス属性の決定について
UNIX上のアクセス属性について基本的にはファイルの所有者、所有者のプライマリグループ、Everyoneが持つWindows上のアクセス権をもとに決定しますが、単純にUNIX上の所有者、グループメンバ、その他のアクセス属性に一対一に対応させるわけではありません。
例えば所有者のアクセス属性の決定には所有者だけでなくEveryoneのアクセス権も考慮します。同様にグループメンバのアクセス属性の決定には所有者のプライマリグループだけでなくEveryoneのアクセス権も考慮します。

上記のルールに従ってアクセス権のマッピングが行われるため、UNIX からファイルを作成する場合には、UNIX 上で見えるアクセス権と Windows 上のアクセス権はほぼ一致していますが、Windows 上から作成する場合は、Windows 上で見えるアクセス権と UNIX 上で見えるアクセス権は一致しないことがありますので、注意が必要です。

■ ユーザーマッピングに関する例
ファイルグループ（プライマリグループ）はUNIXからファイルを作成するとマッピングされたグループ名が設定されますがWindowsから作成した場合、通常ローカルユーザーではNULLが、ドメインユーザーではそのユーザーのプライマリグループが設定されます。

■ アクセス属性に関する例

Windows上からファイルを作成した場合にUNIX上で見えるアクセス権の設定例を、いくつかパターンを挙げ説明します。

(パターン１)

Windows 上のファイルのアクセス権：Everyone → フルコントロール

UNIX 上のファイルのアクセス権　：ファイルの所有者 → rwx

所有者のグループ → rwx

その他のグループ → rwx

ファイルの所有者、所有者のグループのアクセス権を設定する為にEveryoneのアクセス権も考慮されている為。

(パターン２)

Windows 上のファイルのアクセス権：ファイルの所有者 → 読み取りと実行、読み取り

ファイルグループ → 読み取りと実行、読み取り

Everyone → フルコントロール

UNIX 上のファイルのアクセス権　：ファイルの所有者 → rwx

所有者のグループ → rwx

その他のグループ → rwx

ファイルの所有者、所有者のグループのアクセス権を設定する為にEveryoneのアクセス権も考慮されている為。

(パターン３)

Windows 上のファイルのアクセス権：ファイルの所有者 → フルコントロール

ファイルグループ → フルコントロール

Everyone → 読み取りと実行、読み取り

UNIX 上のファイルのアクセス権　：ファイルの所有者 → rwx

所有者のグループ → rwx

その他のグループ → r-x

その他のグループのアクセス権の設定には、ファイルの所有者(Windows上)、所有者のグループ(Windows上)のアクセス権は考慮されない為。

このようなアクセス権の違いを解決する為に必要に応じてファイルの所有者、グループ、アクセス権を変更する必要があります。

ファイルの所有者、グループ、アクセス権を変更する場合は、以下のコマンドを UNIX クライアントより変更権限のあるユーザーにて行ってください。

- 所有者の変更
  chown [設定するユーザー名] [変更するファイルパス]
- グループの変更
  chgrp [設定するグループ名] [変更するファイルパス]
- アクセス権の変更
  chmod [設定するアクセス権] [変更するファイルパス]

8.1.5 ユーザー/グループマッピングが正しく行われたかを確認するには

マッピングされたユーザー/グループは以下の方法で確認できます。設定が正しくない場合は、マッピングしなおしください。

■ コマンドプロンプトによる確認

1. WebUI の[メンテナンス] - [リモートデスクトップ]をクリックします。
2. ログオン画面が表示されたら、管理者のユーザー名、パスワードを入力し、ログオンします。
3. リモートデスクトップ画面の[スタート]-[すべてのプログラム]-[アクセサリ]-[コマンド プロンプト]を選択し、Command Prompt 画面を起動します。
4. 以下のコマンドを入力し Enter キーを押します。
5. mapadmin list –all
6. マッピングされているユーザーとグループの一覧が表示されます。
7. 確認が終わったら Command Prompt 画面を終了し、リモートデスクトップをログオフします。

■ Services for UNIX Administration画面での確認

1. WebUI の[メンテナンス] - [リモートデスクトップ]をクリックします。
2. ログオン画面が表示されたら、管理者のユーザー名、パスワードを入力し、ログオンします。
3. リモートデスクトップ画面で[スタート]-[すべてのプログラム]-[Windows Services for UNIX] -[Services for UNIX Administration]を選択します。
4. 画面左のツリー中の[User Name Mapping]をクリックします。
5. 画面右の[Maps]をクリックします。
6. [Show User Maps]をクリックします。
7. 画面下の[Display simple maps in Mapped users list]のチェックボックスをクリックします。
8. [Mapped users:]リストボックスに簡略および明示的にマッピングされているユーザー一覧が表示されます。
9. 同じように、マッピングされたグループ一覧を表示させるには、手順 5 で開いた画面で[Show Group Maps]をクリックします。
10. 画面下の[Display simple maps in Mapped groups list]のチェックボックスをクリックします。
11. [Mapped groups:]リストボックスに簡略および明示的にマッピングされているグループの一覧が表示されます。
12. 確認が終わったら Services for UNIX Administration 画面を終了し、リモートデスクトップ画面をログオフします。

8.1.6　　ドメインコントローラの設定について

iStorage NS がドメインに参加している場合、そのドメイン内のすべてのドメイン コントローラに NFS 認証サーバをインストールする必要があります。また、UNIX 側が NIS でユーザ情報を管理している場合、Server for NIS をドメインコントローラにインストールすることにより、Windows ユーザと UNIX ユーザを一元管理することができます。

Windows NT ドメイン環境にて使用される場合は WindowsNT4.0 with Service Pack 6a 及び Microsoft Internet Explorer 5.0 以降にアップグレードしておく必要が有ります。
インストールを行う前に以下のモジュールをダウンロードし、インストールしておく必要が有ります。
http://download.microsoft.com/download/platformsdk/wmix86/1.1/W9XNT4/EN-US/wbemcore.exe
http://download.microsoft.com/download/WindowsInstaller/Install/2.0/NT45/EN-US/InstMsiW.exe
http://www.microsoft.com/japan/windows2000/server/evaluation/news/bulletins/adextension.asp
(2006 年 3 月 29 日現在)
Server for NIS は Active Directory を使用しておりますので Windows NT ドメインコントローラでは使用できません。

8.1.6.1　　NFS認証サーバ

NFS ユーザーの認証にドメイン アカウントが使用される場合（NFS サーバのユーザーが Windows ドメイン ユーザーにマップされている場合）は、すべての認証を行うコンピュータ（ドメイン コントローラおよびバックアップ ドメイン コントローラ）に NFS 認証サーバをインストールする必要があります。
Windows ドメイン ユーザーにマップする場合は、次頁のように構成してください。
ただし、以下の条件をすべて満たす場合、認証サーバをドメインコントローラにインストールする必要はありません。

- ドメイン内のすべてのドメインコントローラが Windows 2003 である。
- ドメイン内のすべての iStorage NS にインストールされている SFU のバージョンが3.5である。

iStorage NS では、モデルによって SFU のバージョン 3.0 またはバージョン 3.5 をサポートしています。
SFU のバージョン 3.0 をサポートしているモデルは下記となり、列挙されていないモデルは SFU のバージョン 3.5 をサポートしているモデルです。
Windows Server 2003（NS23P/NS43P/NS44P/NS130/NS240/NS430/NS440/NS510G/NS520G）

1. 各 Windows ドメインコントローラに、NFS 認証サーバをインストールします。
   NFS 認証サーバには、設定オプションはありませんので、個別の設定は不要です。 (ユーザー名マッピングはインストールしません。)

2. WebUI で iStorage NS に接続し、ユーザー名マッピングを構成します。
   Windows ドメイン内に iStorage NS が複数台存在する場合は、ユーザー名マッピングを構成する iStorage NS は 1 台のみでかまいません。各 iStorage NS では、[User Mapping/Computer Name] に、ユーザー名マッピングを構成した iStorage NS のコンピュータ名を指定します。これは WebUI から設定できないため[メンテナンス]－[リモートデスクトップ]で[スタート]－[プログラム]－[Windows Services for UNIX]－[Services for UNIX Administration]を起動し Server for NFS の User Mapping タブの Computer Name に設定します。
   - 補足
   ユーザー名マッピングは、Windows グループ/ユーザーの情報と、UNIX グループ/ユーザーの情報を結合し、マッピングするもので、これ自体では認証は行いません。
   Windows グループ/ユーザーの情報は Windows ドメインコントローラから、UNIX グループユーザーの情報は、NIS サーバ、あるいは PCNFS サーバから取得します。
3. iStorage NS で、NFS サーバを適宜に構成します。

8.1.6.2 Server for NIS

ドメインコントローラに Server for NIS をインストールした場合、NIS ドメインが Windows のドメインと統合され、Active Directory を使用して両方のドメインを管理できます。これによりシステム管理者はユーザー情報、グループ情報といった UNIX、Windows の共通情報、また UNIX のみで使用可能な NIS 情報も Windows 側のみで管理出来るようになります。

8.1.6.3 ドメインコントローラの設定

ドメインコントローラに Server for NIS をインストールする場合は「Server for NIS を使用する場合の設定」を、Server for NIS をインストールしない場合は「Server for NIS を使用しない場合の設定」をそれぞれ参照し、ドメインコントローラの設定を行ってください。

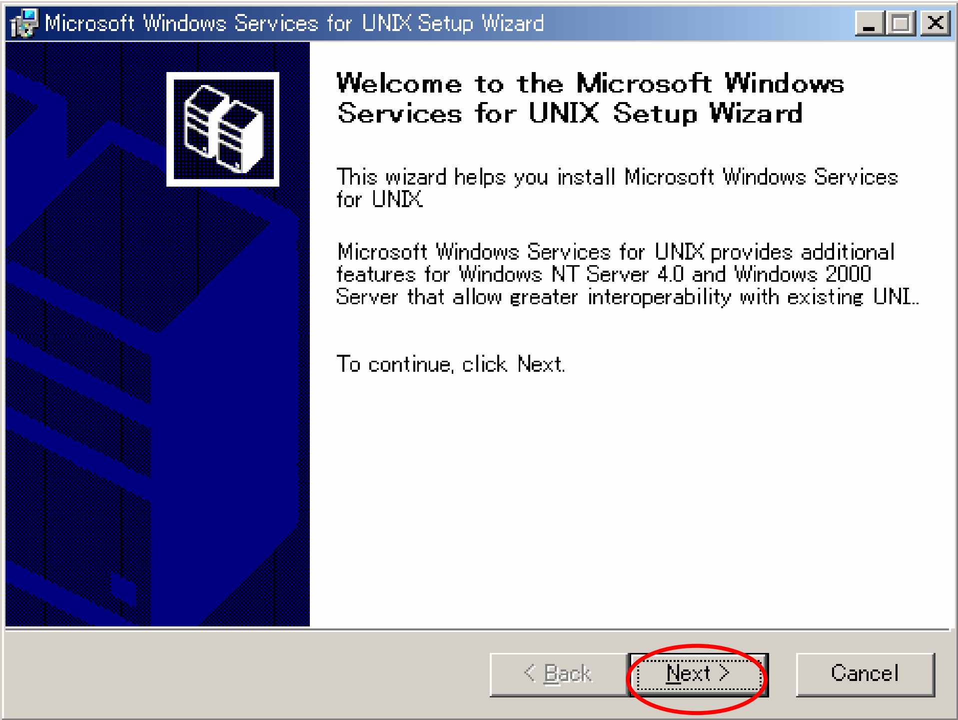
4. **Server for NIS** を使用する場合

（1）**Server for NIS**及び**NFS**認証サーバ インストール手順

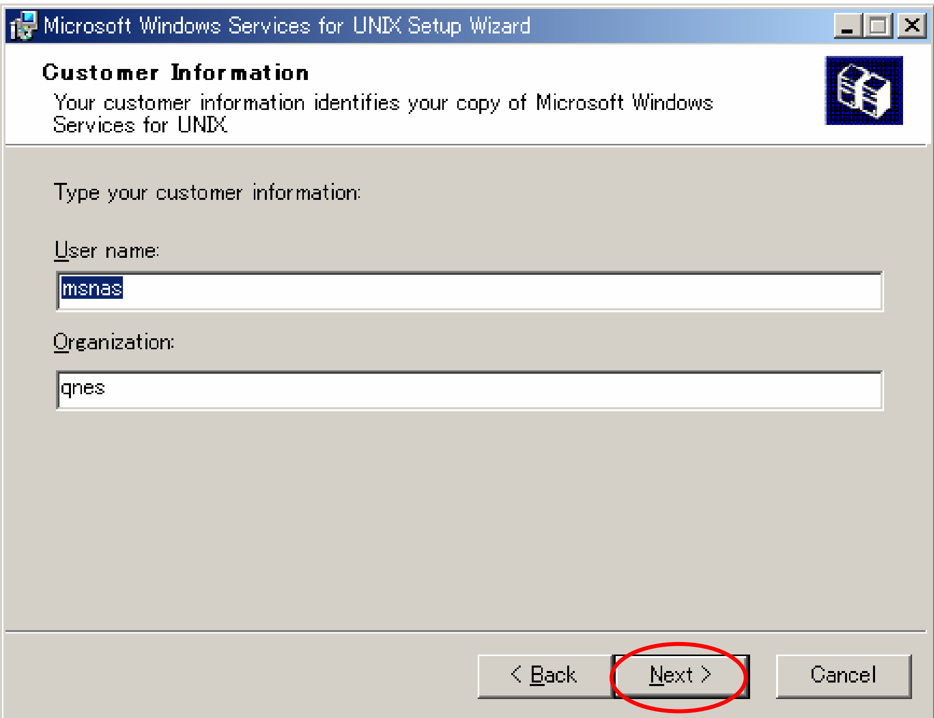
① EXPRESSBUILDER(SE)CD-ROM より、Sfu30 または Sfu35 フォルダにある OEMSetup.msi を起動します。

② このソフトウェアは、次世代のインストールファイル msi パッケージにて配布しており、ドメインコントローラの状態によっては OEMSetup.msi を起動できない場合があります。同一フォルダ内にある InstMsi.exe を起動し、Windows Installer のインストールを行ってください。

③ [Microsoft Windows Services for UNIX Setup Wizard]が起動しますので、[Next]をクリックします。



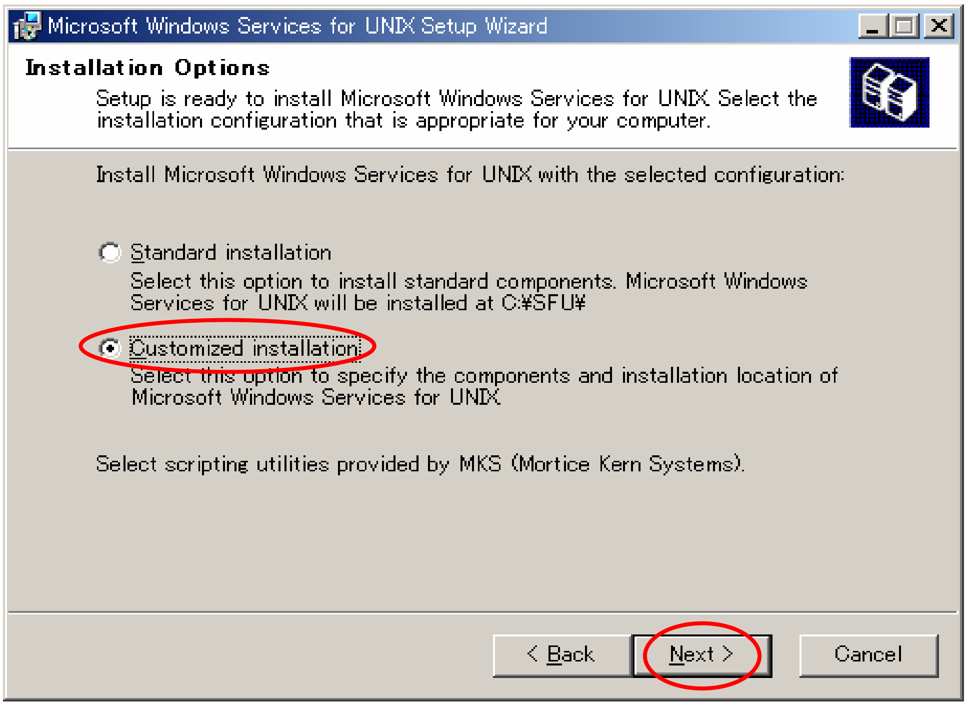
④ [Customer Information]では特にデフォルトの設定で問題なければ[Next]をクリックします。



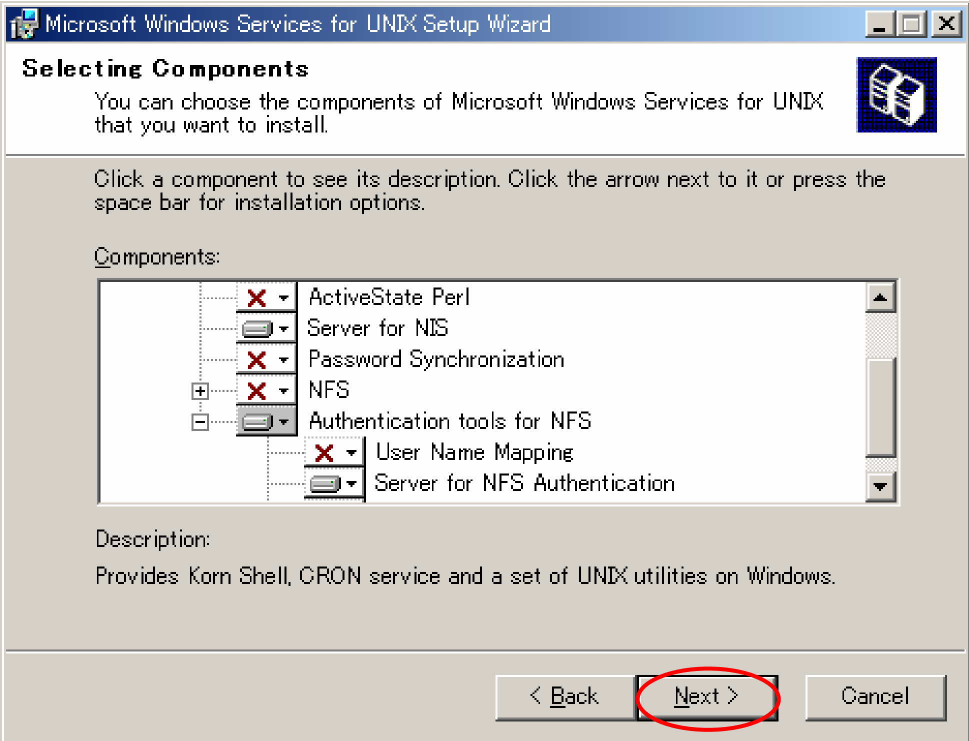
⑤ [License and Support Information]では[End-User License Agreement]の内容に特に問題がなければ[I accept the agreement]を選択し、[Next]をクリックします。



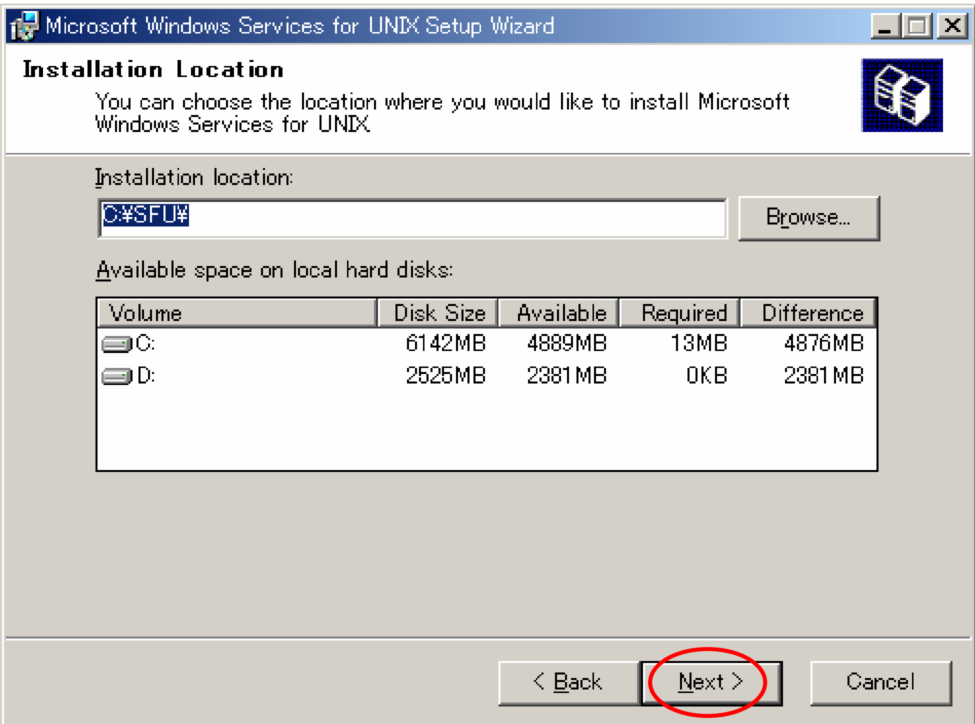
⑥ [Installation Options]では[Customized installation]を選択し、[Next]をクリックします。



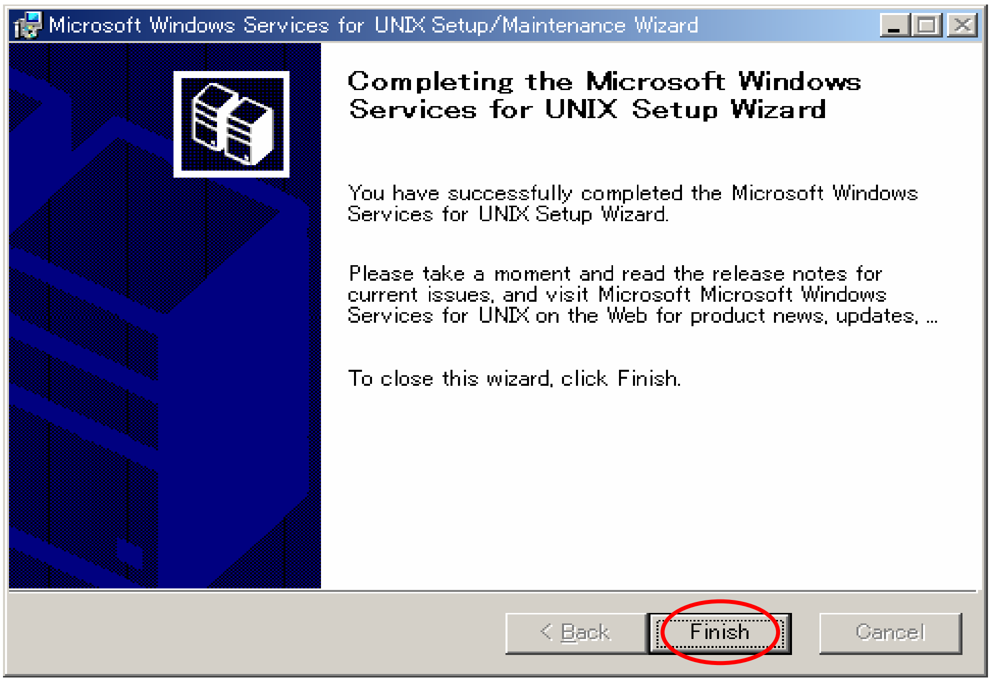
⑦ [Selecting Components]では[Server for NIS]と[Password Synchronization]と[Authentication tools for NFS]-[Server for NFS Authentication]の設定を[Will be installed on local hard drive]に変更し、上記以外の項目で [Will be installed on local hard drive]がデフォルト設定されている項目はすべて[Entire feature will not be available]を設定し[Next]をクリックします。



⑧ [Installation Location]では特に問題がなければデフォルトの設定のまま[Next]をクリックします。

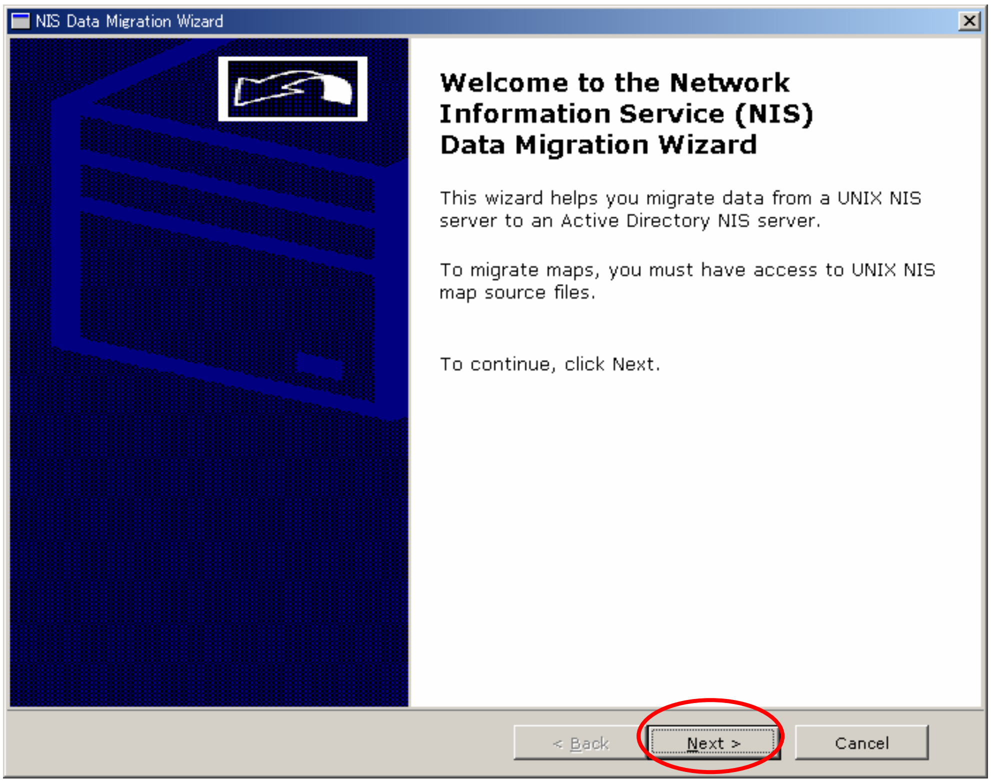


⑨　インストールが完了すると以下の画面が表示されるので、[Finish]をクリックし、インストール画面を終了します。



（2）**Server for NIS 設定手順**

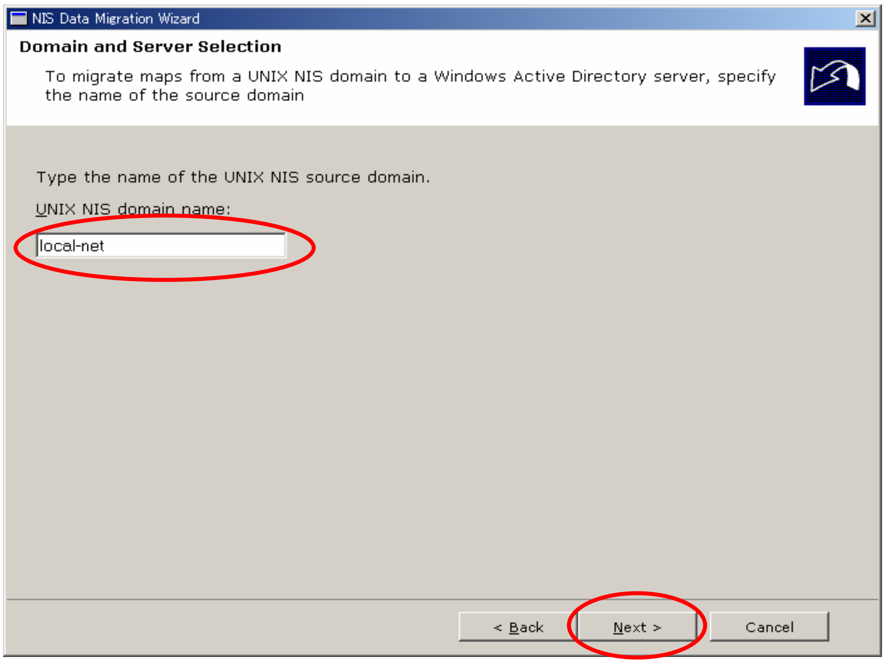
1. スタートメニューより[プログラム]-[Windows Services for UNIX]-[NIS Server Migration]を選択します。
2. [Welcome to the Network Information Service(NIS) Data Migration Wizard]が起動されますので、[Next]をクリックします。



3. [Domain and Server Selection]では、NIS 情報を移行する場合のみ、NIS ドメイン名を入力し、[Next]をクリックします。

・ 既存のNISドメインを移行する場合は、移行するNISドメイン名を入力してください。

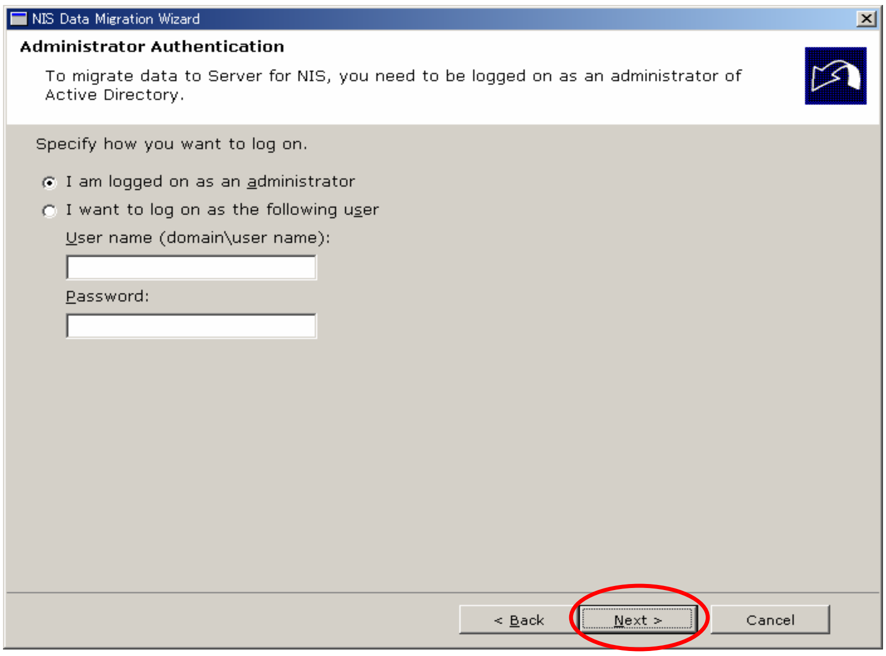
・ NISドメインを新たに作成する場合は、[UNIX NIS domain name]には何も入力しないでください。



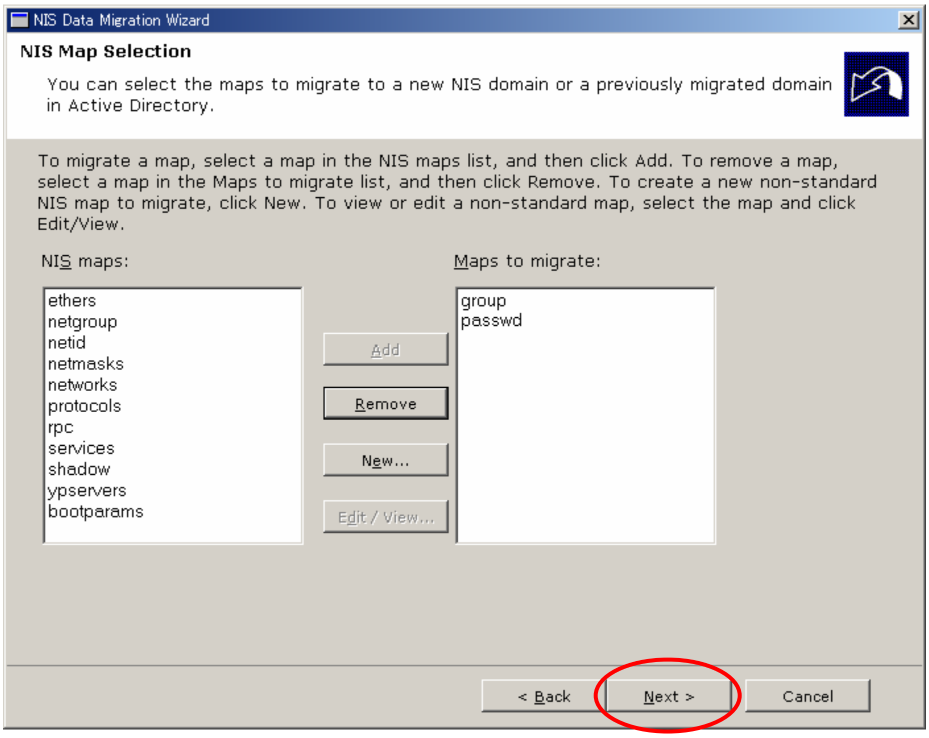
4. [Administrator Authentication]では、Active Directory の管理者を指定し、[Next]をクリックします。

・ 管理者が[Administrator]の場合は[I am logged on as an administrator]を選択します。

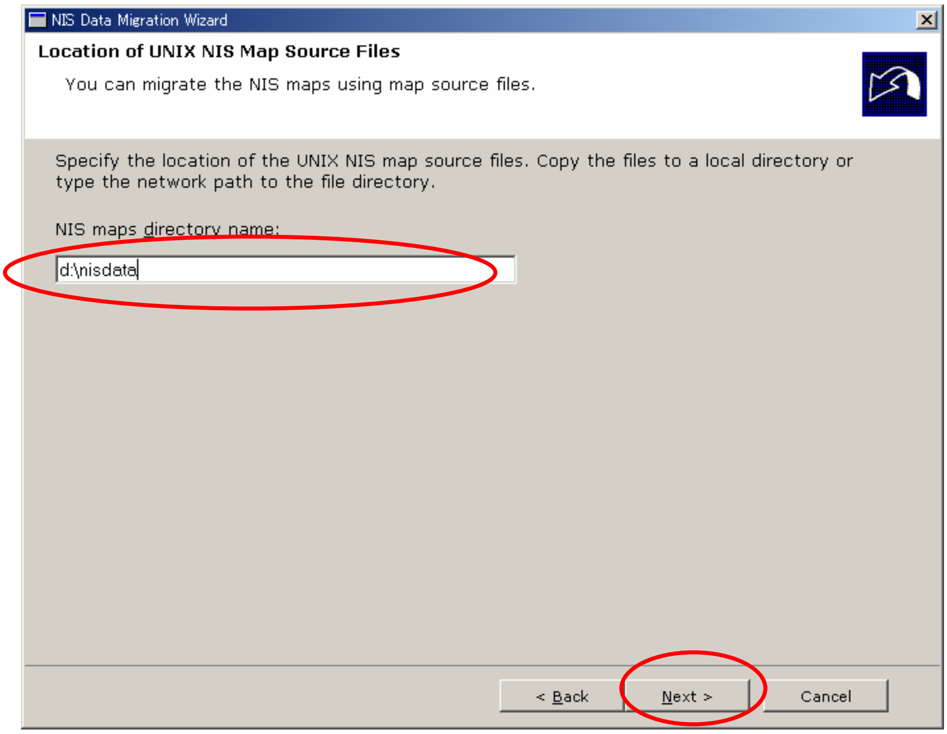
・ 管理者が[Administrator]以外の場合は[I want to log on as the following user]を選択し、管理者の[user name]と[password]を入力します。



5. [NIS Map Selection]では、移行するマップを選択し、 [Next]をクリックします。
「passwd」と「group」は必ず移行してください。その他のマップについては任意に指定します。

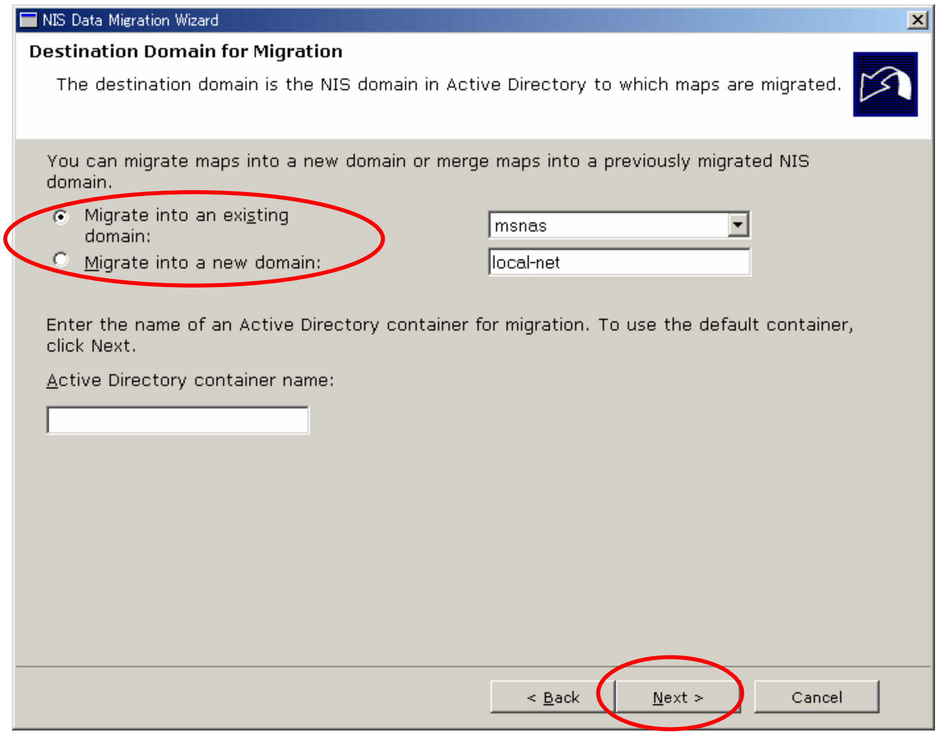


6. [Location of UNIX NIS Map Source Files]では、移行するマップのソースファイルを選択し、 [Next]をクリックします。(移行するソースファイルはあらかじめ Windows 側へ転送しておく必要があります。)



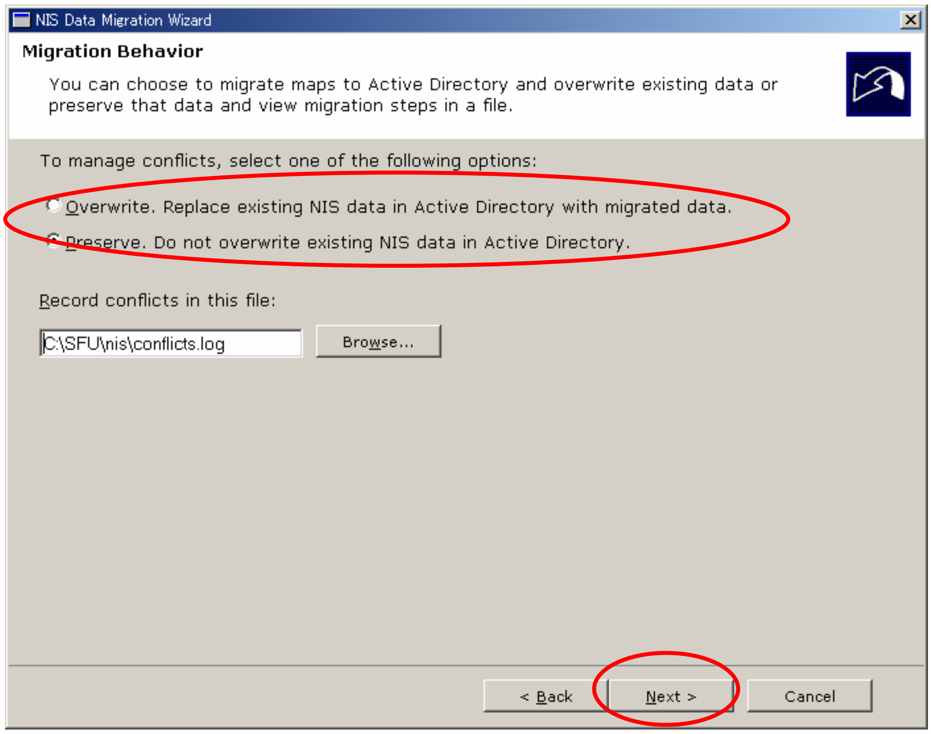
7. [Destination Domain for Migration]では、移行するドメインを設定し、 [Next]をクリックします。

- Windows既存のドメインをNISドメインとして使用する場合は、[Migrate into an existing domain]を選択します。
- UNIX既存のドメインをそのまま使用する場合は、[Migrate into a new domain]を選択します。

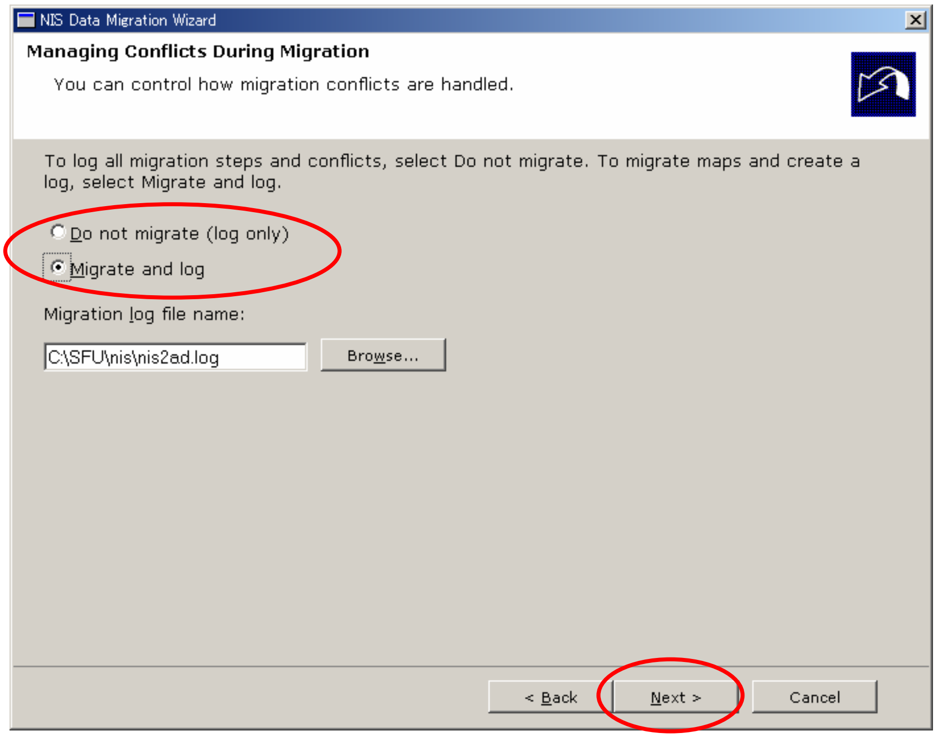


8. [Migration Behavior]では､移行するユーザーデータが Windows のユーザー情報と競合した場合の設定を行い、 [Next]をクリックします。

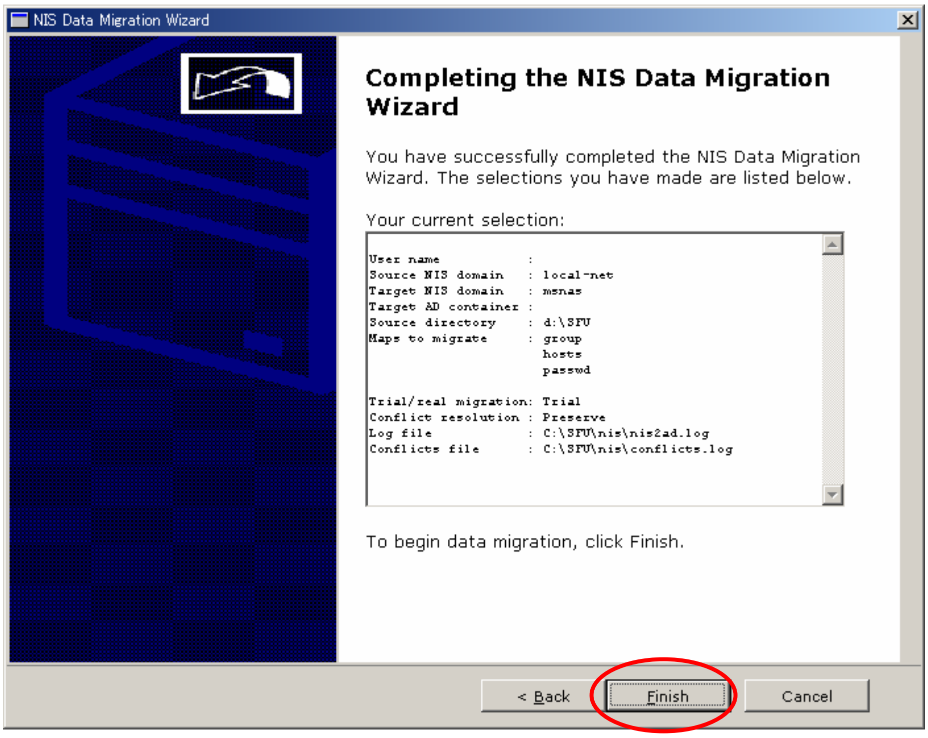
- 移行するユーザーデータがWindowsのユーザー情報と競合した場合、既存のWindowsのユーザー情報を上書きする場合は、[Overwrite、 Replace existing NIS data in Active Directory with migrated data]を選択します。
- 移行するユーザーデータがWindowsのユーザー情報と競合した場合、既存のWindowsのユーザー情報を保持する場合は、[Preserve, Do not overwrite existing NIS data in Active Directory]を選択します。



9. [Managing Conflicts During Migration]では、[Migrate and log]を選択し、 [Next]をクリックします。



10. [Completing the NIS Data Migration Wizard]では設定内容に問題なければ [Finish]をクリックします。

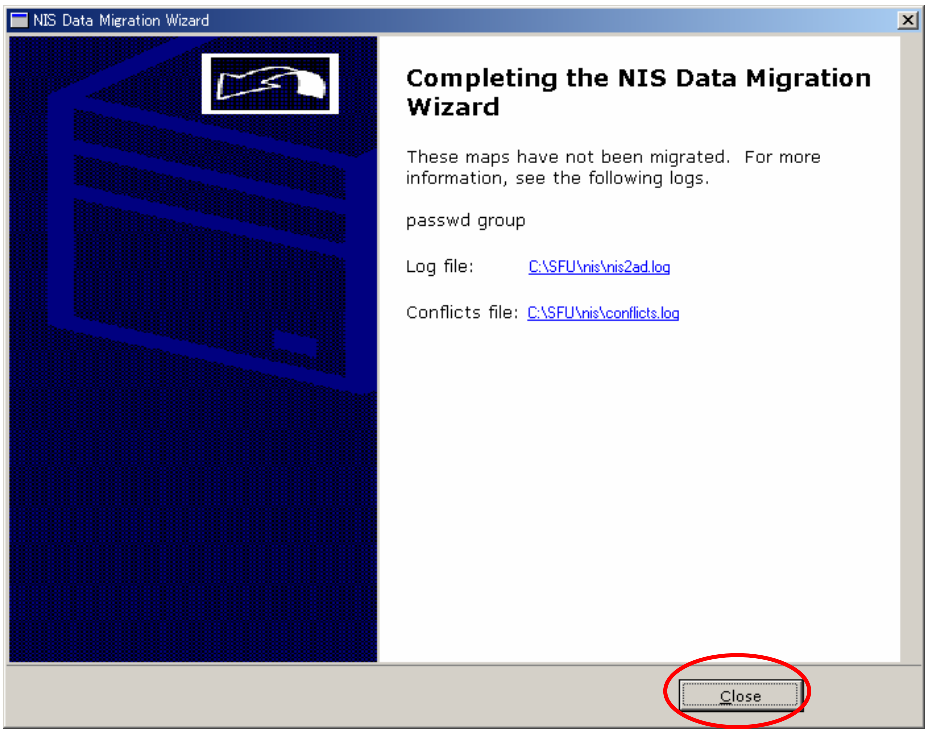


11. [Completing the NIS Data Migration Wizard]では実行結果のログファイルを参照出来ます。

問題が無ければ、[close]を選択します。

log file：移行結果のログ情報ファイル

conflicts file：競合結果の情報ファイル



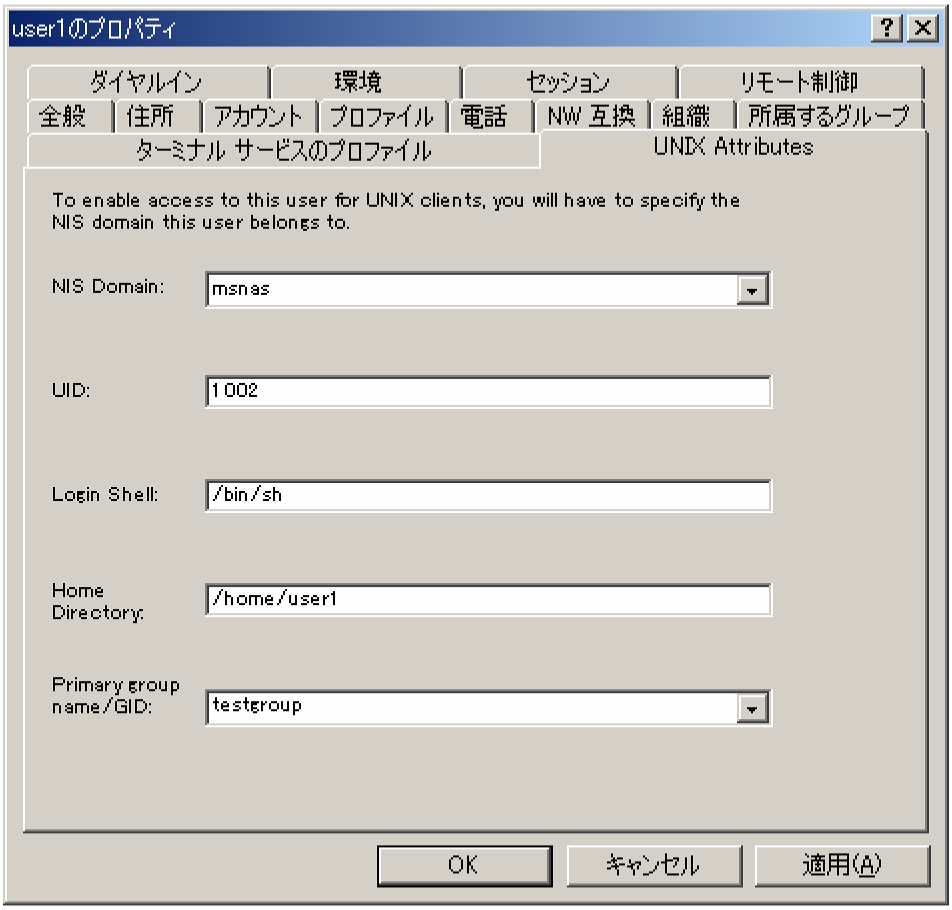
(3) NIS オブジェクトの管理

NIS オブジェクトの管理は、Active Directory の標準管理ツールを使用して行います。

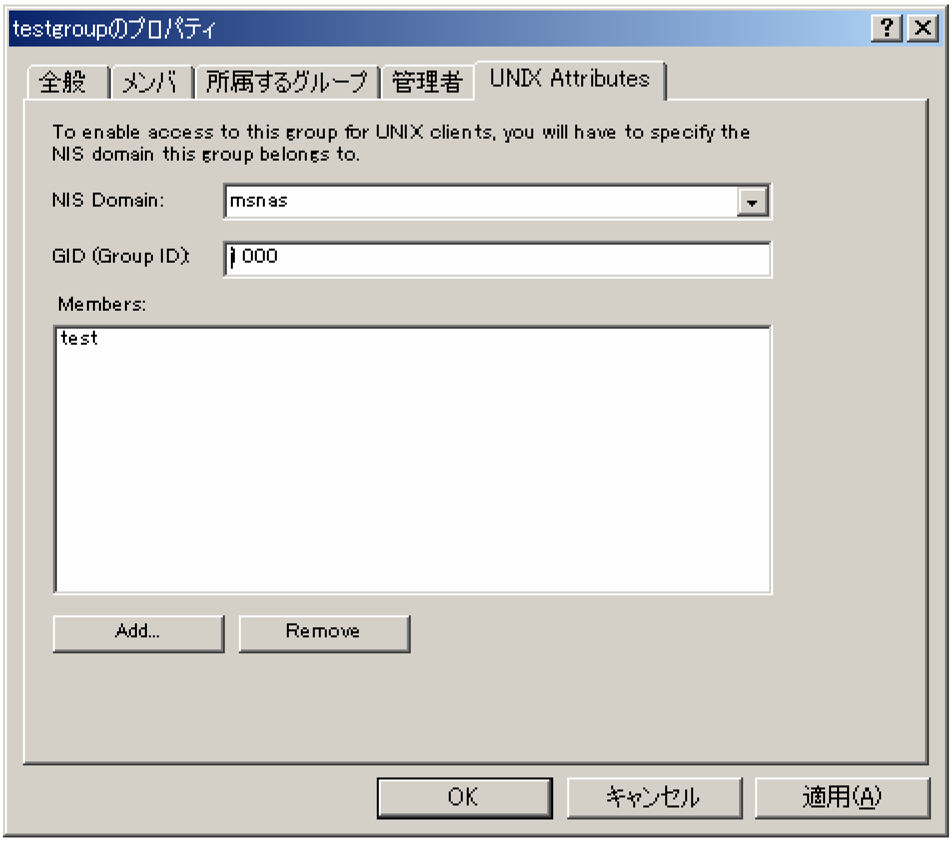
① スタートメニューより[プログラム]-[管理ツール]-[Active Directory ユーザーとコンピュータ]を選択します。

② [Active Directory ユーザーとコンピュータ]が起動しますので、任意のユーザーまたはグループを選択し、プロパティを選択します。

③ ユーザーのプロパティ画面より[UNIX Attributes]タブを選択し、ユーザー情報を設定します。



④ グループのプロパティ画面より[UNIX Attributes]タブを選択し、グループ情報を設定します。



12. **Server for NIS** を使用しない場合

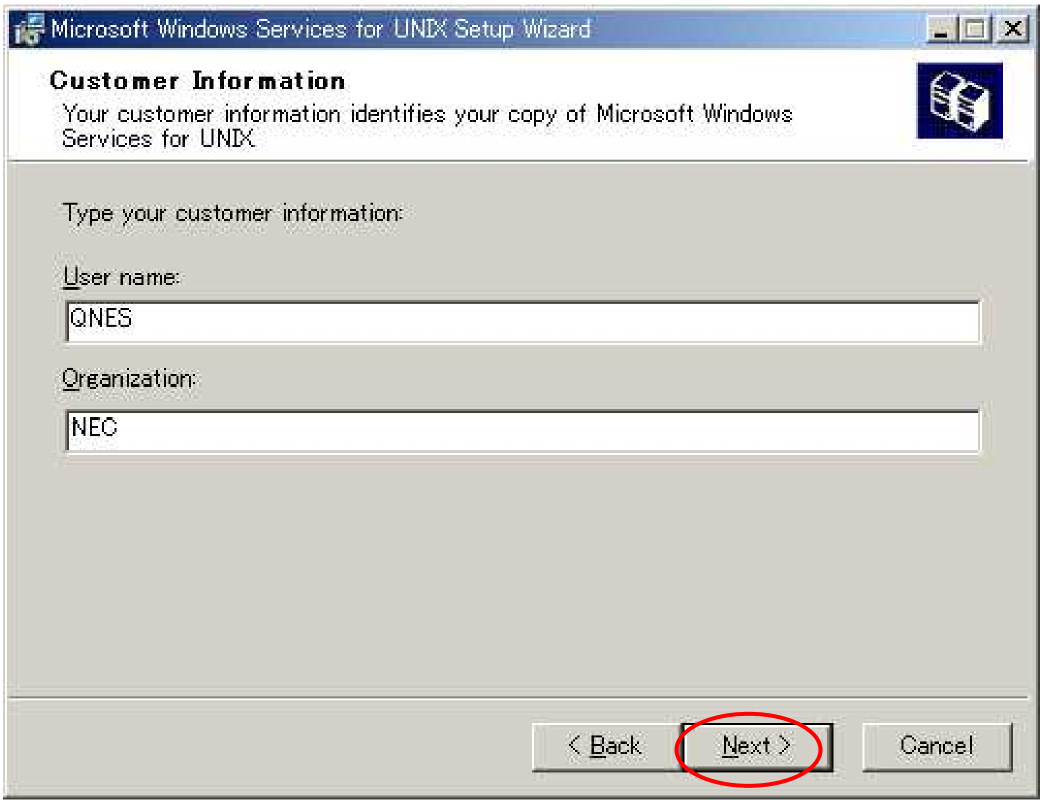
(1) **NFS** 認証サーバインストール手順

① EXPRESSBUILDER(SE)CD-ROMより、Sfu30またはSfu35フォルダにあるsfucustom.msiを起動。
※このソフトウェアは、次世代のインストールファイル msi パッケージにて配布しており、ドメインコントローラの状態によってはsfucustom.msiを起動できない場合があります。同一フォルダ内にあるInstMsi.exeを起動し、Windows Installerのインストールを行ってください。

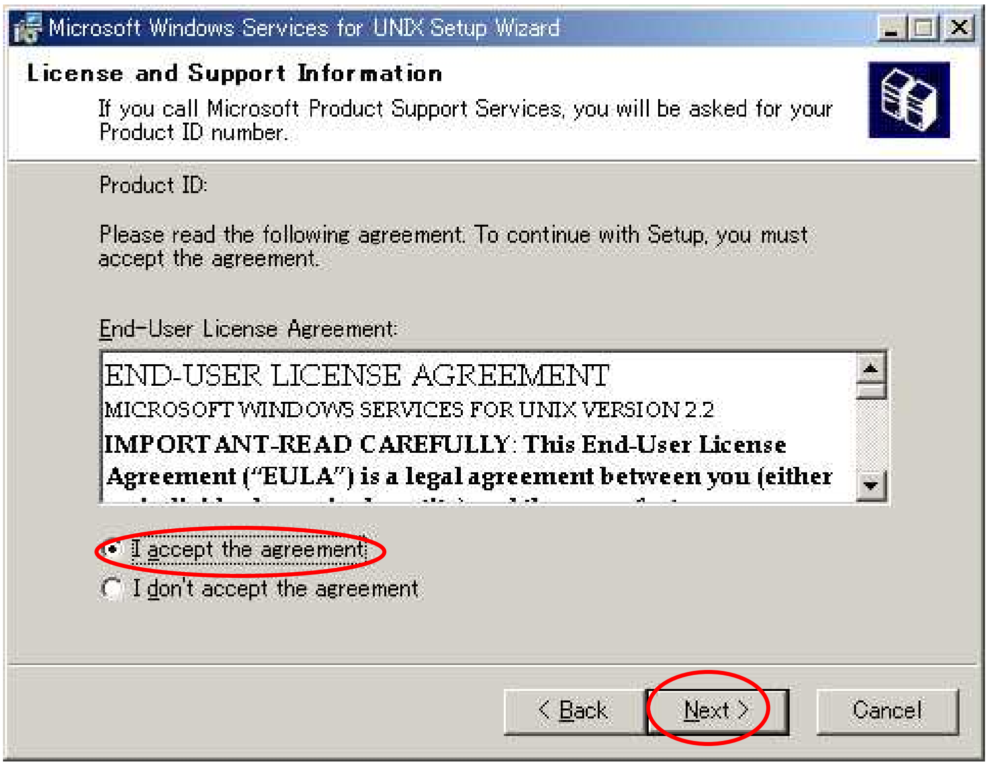
② [Microsoft Windows Services for UNIX Setup Wizard]が起動するので、[Next]をクリックする。



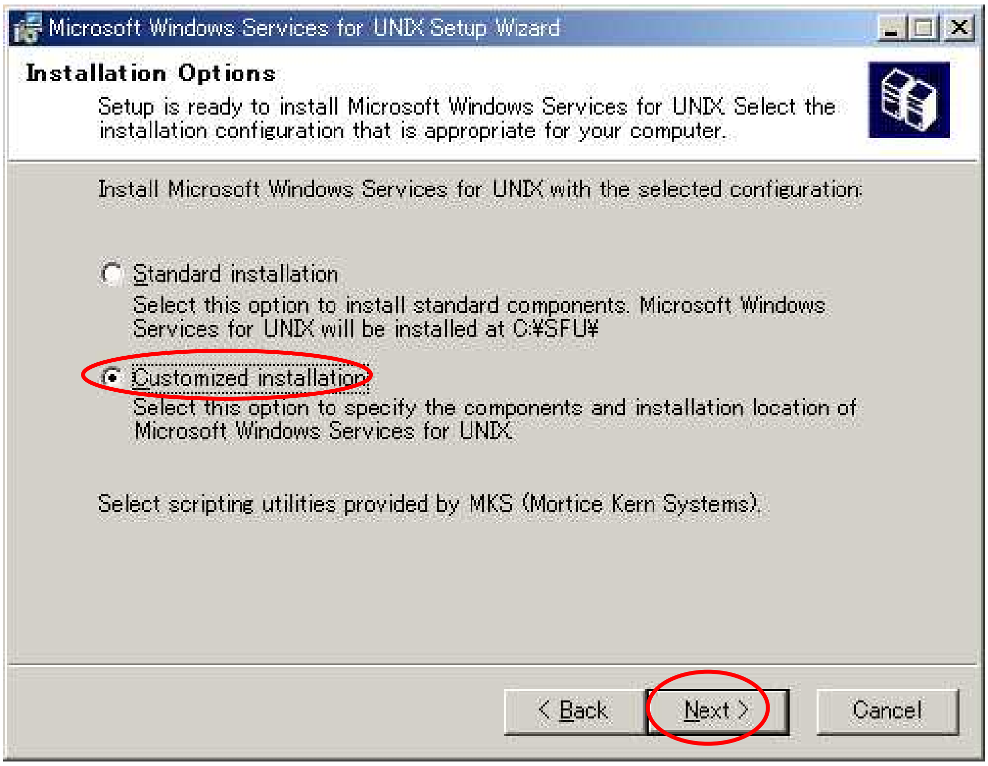
③ [Customer Information]では特にデフォルトの設定で問題なければ[Next]をクリックする。



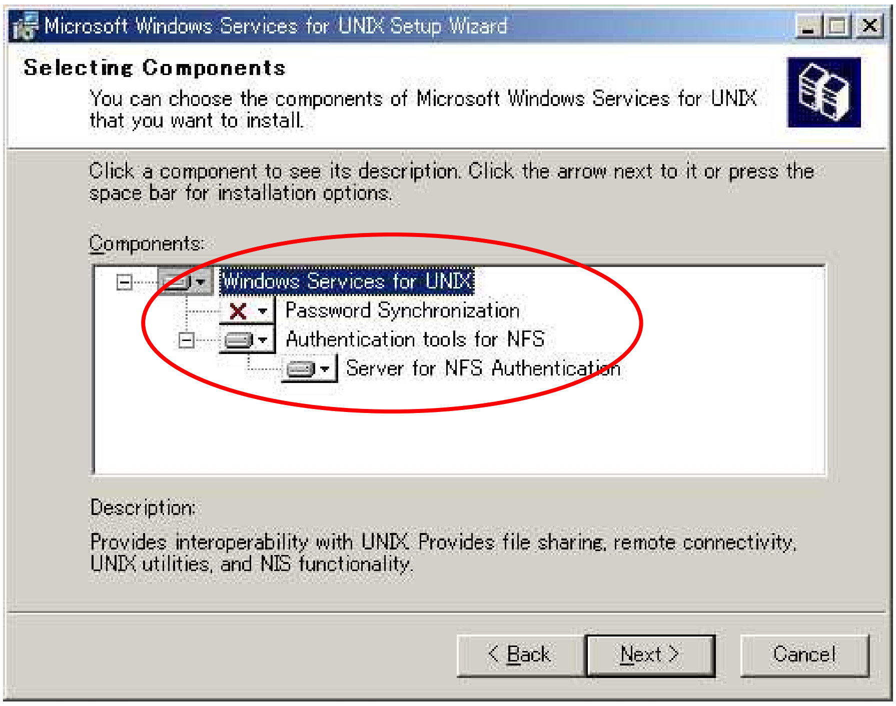
④ [License and Support Information]では[End-User License Agreement]の内容に特に問題がなければ[I accept the agreement]を選択し、[Next]をクリックする



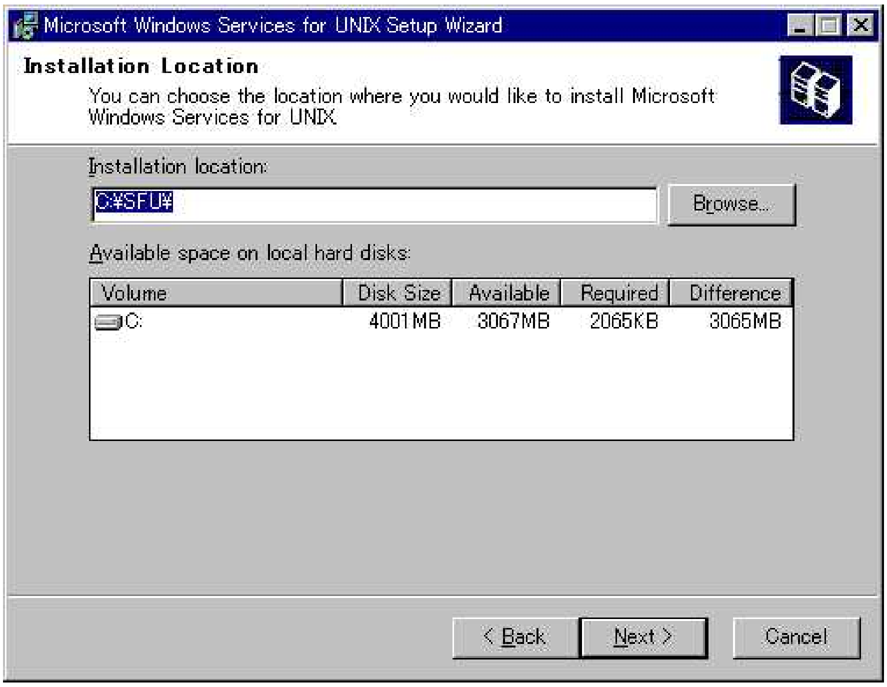
⑤ [Installation Options]では[Customized installation]を選択し、[Next]をクリックする。



⑥ [Selecting Components]では[Password Synchronization]の設定を[Entire feature will not be available]に変更し、上記以外の項目で [Will be installed on local hard drive]がデフォルト設定されている項目はすべて[Entire feature will not be available]を設定し、設定が以下のようになっていることを確認し、[Next]をクリックする。



⑦ [Installation Location]では特に問題がなければデフォルトの設定のまま[Next]をクリックする。



⑧ インストールが完了すると以下の画面が表示されるので、[Finish]をクリックし、インストールを終了する。



8.1.7 UNIXユーザー設定に関する注意事項

- 下記のWindowsユーザーにUNIXユーザーをマッピングした場合には正常にマッピング動作が働かない場合があります。これらのWindowsユーザーにはマッピングしないでください。
- Guest, IUSR_NEC-NAS, IWAM_ NEC-NAS
- ユーザー名とグループ名には日本語は使えません。
- [簡易マッピング]を使用した場合、WindowsとUNIXで同一のユーザー名やグループ名がある場合は、iStorage NSはそれらのグループやユーザーに対して暗黙のマッピングを作成しますので、それらについては[明示的なユーザーマッピング]または[明示的なグループマッピング]を行わないでください。行った場合は正常にマッピング動作が働かない場合があります。
- [明示的なユーザマッピング]および[明示的なグループマッピング]でNISサーバを使用したマッピングと、[パスワードファイルとグループファイル]を使用したマッピングを同時に使用することはできません。マッピングに使用する参照先を変える場合は、以前に作成した明示的なマッピングをあらかじめ削除してください。
- NISサーバを使用したマッピングを行うと、iStorage NSは定期的にNISサーバにアクセスします。このため、NISサーバにアクセス出来ないような状況が発生すると、エラーをイベントログに出力します。
- 一部のUNIXのバージョンまたはUNIX互換OSが持つNISサーバの機能にはiStorage NSと互換が無い場合があります。NISサーバを指定して、[UNIXグループの一覧]または[UNIXグループの一覧]に一覧を表示できない場合はパスワードファイルとグループファイルを使用する設定に変更してください。
- 設定したマッピングがすぐには反映されない場合があります。このような場合はiStorage NSを再起動すると反映されます。
- 700以上のユーザー、グループを取り扱う場合はWebUIで設定ができない場合があります。以下の手順で行ってください。

  (1) WebUIの[メンテナンス]—[リモートデスクトップ]をクリックします。

  (2) ログオン画面が表示されたら、管理者のユーザー名、パスワードを入力し、ログオンします。

  (3) 管理者メニューより [Services for UNIX Administration]を起動し、[User Name Mappings]の[Maps]タブにて設定を行います。

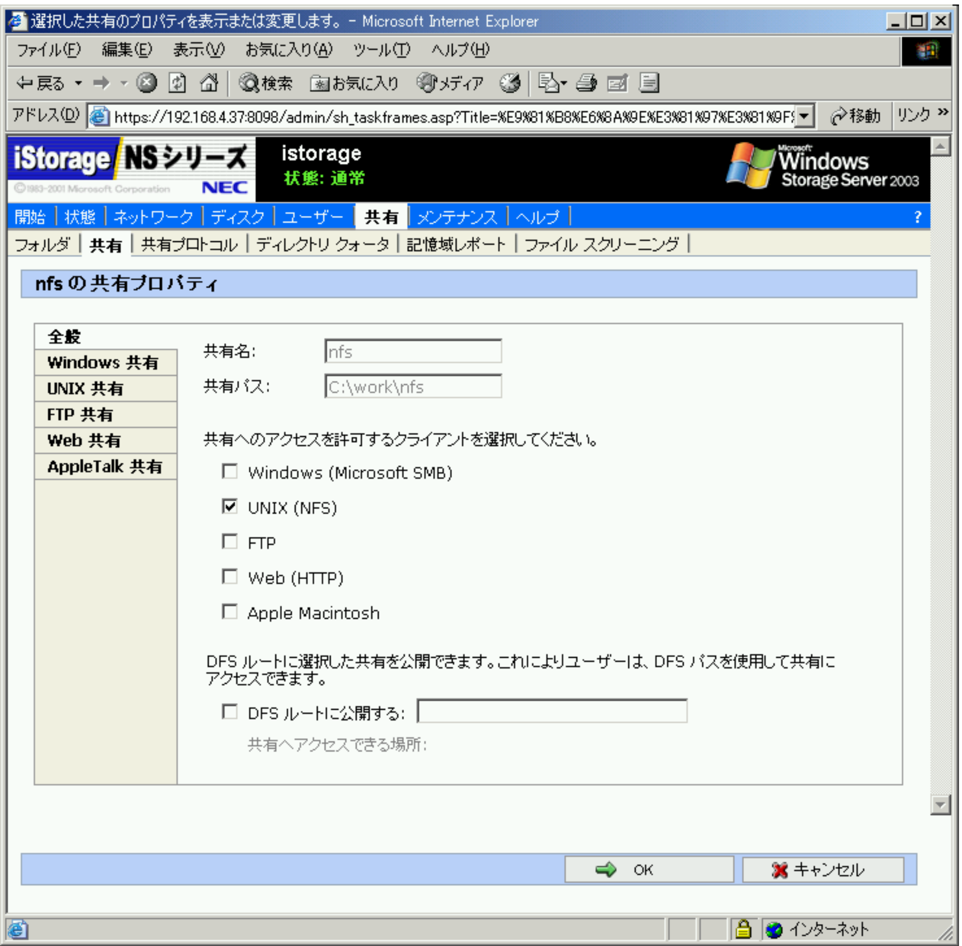
  (4) [Services for UNIX Administration]を終了し、リモートデスクトップ画面をログオフします。

8.2　NFSによる共有

iStorage NS からクライアントへ公開する“共有”を設定します。クライアントがアクセスするための共有名と、その共有を iStorage NS 内のどのフォルダに作成するかを指定します。工場出荷時にはユーザー領域として使用できる共有を定義していません。新たに共有を定義して使用を開始してください

共有を作成するには、以下の手順で行います。

1. WebUI の[共有]→[共有]をクリックします。
2. [新規]を選択します。
3. [全般]タブで[共有名]、[共有パス]、アクセスを許可するクライアント[UNIX(NFS)]を指定します。
4. 選択したプロトコルのタブをクリックし、それぞれのプロトコル固有の設定を行った後、[OK]ボタンをクリックします。



図．共有の設定

NFSアクセス

UNIX クライアントに対して公開する共有の設定を行います。SMB による共有と比べ、NFS による共有は注意すべきことがいくつかあります。

- ファイルのロック

SMB でのアクセスはロックを保持しますが、NFS の定義ではロックは必須ではありません。つまり、ファイルにロックをかけずに処理を行うアプリケーションもあれば、ロックがかかっているかをチェックせずにファイルの処理を行うアプリケーションもあります。これらの処理をどうするかはアプリケーション、そのファイルを利用するプログラムの処理によるので、Windows 環境と同時に使用する際には注意が必要です。Windows 環境で使用するファイルを同時に NFS で共有し、上記のようなアクセスを行うとファイルを破壊する可能性がありますので、そのような使い方はできません。

また、ファイルにロックがかかった状態で iStorage NS への接続が中断され、再度接続が確立された場合、ロックが解放されてしまう可能性があります。これを防ぐために、クライアントからのロックの再設定要求を一定時間待つ設定をする事で、接続の中断によるロックの解放を防ぎます。待ち時間の指定は、[共有]－[共有プロトコル]で[NFS]の[プロパティ]を選択し、[ロック]選ぶことで設定画面が表示されます。

- 文字コード

Windows 環境と UNIX 環境での文字コードの違いも運用に影響を与える事があります。iStorage NS 上に SMB 経由で日本語のファイル名でファイルを作成した場合、UNIX 環境から NFS 経由でこのファイルが存在するディレクトリを「ls –al」コマンド等で参照すると、日本語のファイル名が正しく表示されない等の問題が起こる可能性があります。これは、UNIX 環境で多く使われている EUC という文字コードと iStorage NS が標準で使用している文字コード体系が異なるためです。そのため日本語のファイル名を、EUC を使用した UNIX 環境で利用する場合は、共有の NFS プロパティを設定する際に[この共有は EUC-JP エンコーディングを使用する]の項目にチェックしてください。

共有を設定する際は、設定した共有に対するアクセス権も必ず設定する事をお勧めします。アクセス権に関しては、8.4.2 NFS 共有のアクセス権の設定の項を参照してください。

・ 隠しファイル属性

Windows 環境でも Unix 環境でもファイルを隠し属性にすることが出来ます。Windows 環境の場合、ファイルを非表示にするには、そのファイルの特殊属性を設定します。UNIX 環境では、ピリオド (.) で始まる名前のファイルはリストされません。iStorage NS の既定では、ピリオドで始まる名前のファイルが Windows ファイル システムの隠しファイル属性として作成されません。ピリオドで始まる名前のファイルを非表示(隠し属性)にするには以下の手順より設定します。

1. 管理 PC の WebUI から[メンテナンス]→[リモートディスクトップ]を起動し iStorageNS へログオンします。
2. 管理者メニューの[Services for UNIX Administration]を選択し、[Server for NFS]を選択します。
3. [Server Settings]のタブを選択し、[File name Handling]の[Create files that have names beginning with '.' as hidden files.]の項目にチェックを入れます。
4. 設定後、画面右上の[Apply]ボタンを押下します。

8.2.1 NFS共有文字変換マッピングについて

Unix 環境では、ファイル名に以下のような特殊文字を使用することがあります。しかし、これらの特殊文字は、Windows のファイルシステムでファイル名として無効な文字と見なします。

特殊文字：(¥),(:),(;),(,),(*),(?),(“),(<),(>),(|)

NFS 共有にてファイル名等にこのような特殊文字をご使用になる場合には、NFS 共有文字変換マッピングの設定が必要です。

NFS 共有文字変換マッピングをご使用した場合、クライアント側では特殊文字のファイル名を使用できます。但し、iStorage NS 上では文字変換テーブルで管理される別の文字を使用し同ファイルを管理します。

例えば、文字変換マッピングを使用し、コロン(:)とアルファベットのＢ(全角)をマッピングしていた場合

－Unix クライアント上では aaa:bb.txt と表示します。

－iStorage NS 上では aaaＢbb.txt と表示します。

8.2.1.1 文字変換マッピングの設定ファイルについて

8.2.1.1.1 文字変換テーブルのフォーマット

文字変換テーブルのフォーマットは以下のような記述となります。

0xnn 0xnn : 0xnn 0xnn [; comment]

nn は、2 バイトの UNICODE の、1 バイト分を、16 進数で指定したものです。

: より前の部分は、UNIX 環境で使用される文字の UNICODE です。

: より後の部分は、Windows 環境で使用される文字の UNICODE です。

; より後の部分は、コメントとなり、無視されます。

- UNIX 環境のコロン(:)と、Windows 環境のハイフン(-)を対応させる場合の例

0x00 0x3a : 0x00 0x2d ; replace client : with - on server

- 注意

ひとつの文字を、二つ以上の文字とマッピングさせないでください。

ピリオド (.) は、マッピングの対象にしないでください。

8.2.1.1.2 設定ファイルのサンプル

以下の情報はサンプルファイルのため、お客様の環境に合わせてファイル内の記述を変更して頂く必要があります。

但し、サンプルファイルをそのままご使用することも可能です。サンプルファイルは以下のように特殊文字をマッピングしています。

――――― ファイル記述例(サンプル) ――――――

0x00 0x5c : 0xff 0x21

0x00 0x3a : 0xff 0x22

0x00 0x2c : 0xff 0x23

0x00 0x3b : 0xff 0x24

0x00 0x2a : 0xff 0x25

0x00 0x3f : 0xff 0x26

0x00 0x22 : 0xff 0x27

0x00 0x3c : 0xff 0x28

0x00 0x3e : 0xff 0x29

0x00 0x7c : 0xff 0x2a

―――――――――――――――――――――

上記サンプルファイルの文字変換マッピング設定内容

(特殊文字をそれぞれ以下のアルファベット(全角)にマッピング)

(¥) → (Ａ)	(?) → (Ｆ)
(:) → (Ｂ)	(") → (Ｇ)
(,) → (Ｃ)	(<) → (Ｈ)
(;) → (Ｄ)	(>) → (Ｉ)
(*) → (Ｅ)	(|) → (Ｊ)

8.2.1.2 文字変換マッピングの設定ファイルの適用手順

1. 管理 PC の WebUI から[メンテナンス]→[リモートデスクトップ]を起動し iStorageNS へログオンします。
2. エクスプローラを起動し、エクスプローラより予め用意した設定ファイルを以下のディレクトリへコピーします。
   C:¥SFU¥table （例では、設定ファイル名を「table」とする。）
3. 管理者メニューの[Services for UNIX Administration]を選択し[Server for NFS]を選択します。
4. [Server Settings]のタブを選択し[File name Handling]の[Translate file names]にチェックを入れます。
5. [Browse…]ボタンを押下し、上記でコピーしたファイル(table)を選択します。
6. 設定後、画面右上の[Apply]ボタンを押下します。
7. 「The settings have been changed successfully. However note that the new settings will take effect only when the server is restarted.」のメッセージダイアログが表示されますので、[OK]ボタンを押下します。
8. 管理者メニューから[サービス]を選択します。
9. 一覧から"server for NFS"をダブルクリックします。
10. [サービスの状態：]で[停止]ボタンを押下します。
11. [サービスの状態：]で[開始]ボタンを押下します。
12. [OK]ボタンを押下します。

8.2.1.3 設定後の確認

NFS 共有文字変換マッピングの設定確認を行います。

1. Unix クライアントより iStorage NS へ NFS 経由でアクセスします。
2. vi、touch コマンドを使用し、特殊文字を使用したファイルを作成します。
3. 管理 PC の WebUI から[メンテナンス]→[リモートデスクトップ]を起動し、ログオンします。
4. エクスプローラ等を使用し、2).で作成したファイル名を参照します。
   ファイル名が文字変換テーブルで管理される別の文字で表示出来ることを確認します。

8.2.2 Windows上での大文字、小文字ファイルの表示

Windows の規定値では、A.txt と a.txt の混在はできません。
大文字、小文字を有効にするためには下記の設定を行う必要があります。

1. WebUI の[メンテナンス]メニューから[リモートデスクトップ]を起動します。
2. 管理者権限のアカウントでログオンします。
3. 管理者メニューから[ローカルセキュリティの設定]を起動します。

4. [セキュリティの設定]→[ローカル ポリシー]→[セキュリティオプション]→[System object:Require case insensitivity for non-Windows subsystems]を選択し、無効に変更します。

📖 NFS 共有についての注意

1. フォルダ名と共有名には日本語を使わないでください。
2. Windows のマウント機能を使用している場合、マウントボリュームを NFS 共有としてアクセスすることはできません。

   マウントされているドライブ配下を NFS で共有する場合は、共有パスにマウント前のディレクトリパスを指定してください。(但し、このような設定にて NFS 共有を行う場合はドライブレーターを使用する必要があります。)

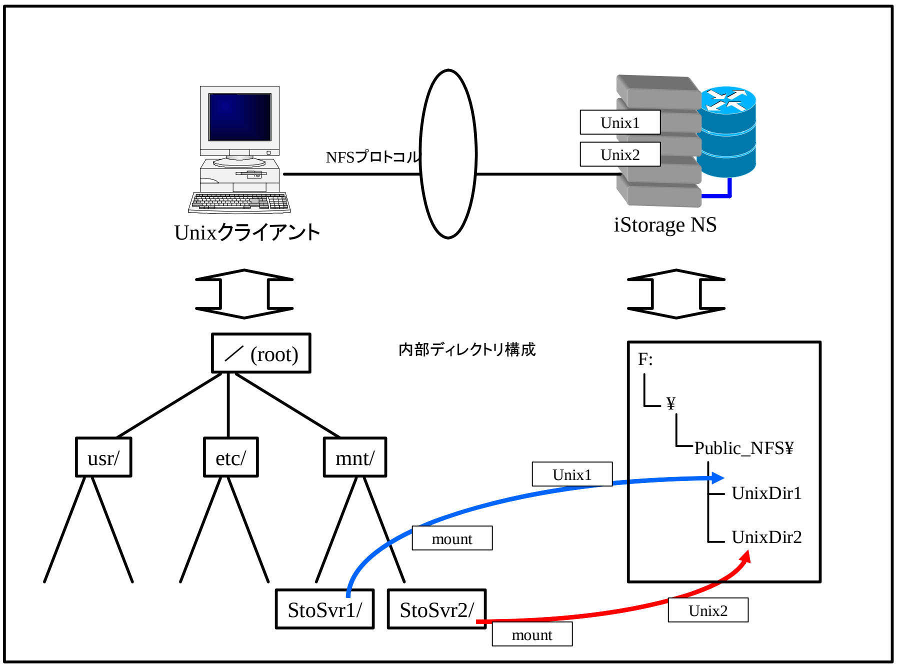
   ※ 例

   F ドライブを E ドライブの NFS ディレクトリにマウントしている場合に、e:¥NFS 配下の sfu ディレクトリを NFS 共有する場合は、「共有パス：」に”f:sfu”と設定します。

   (“e:¥NFS¥sfu”とは設定しないでください。)

8.3　UNIXクライアントからのアクセス（NFS）

UNIX クライアントから iStorage NS 上の NFS による共有へアクセスするには、mount コマンドを使用して、iStorage NS のコンピュータ名と NFS による共有名、クライアントマシン上でのマウントポイントを指定します。mount コマンドの書式については、各 UNIX マシンのオンラインヘルプなどを参照してください。



図．UNIX クライアントからのアクセス

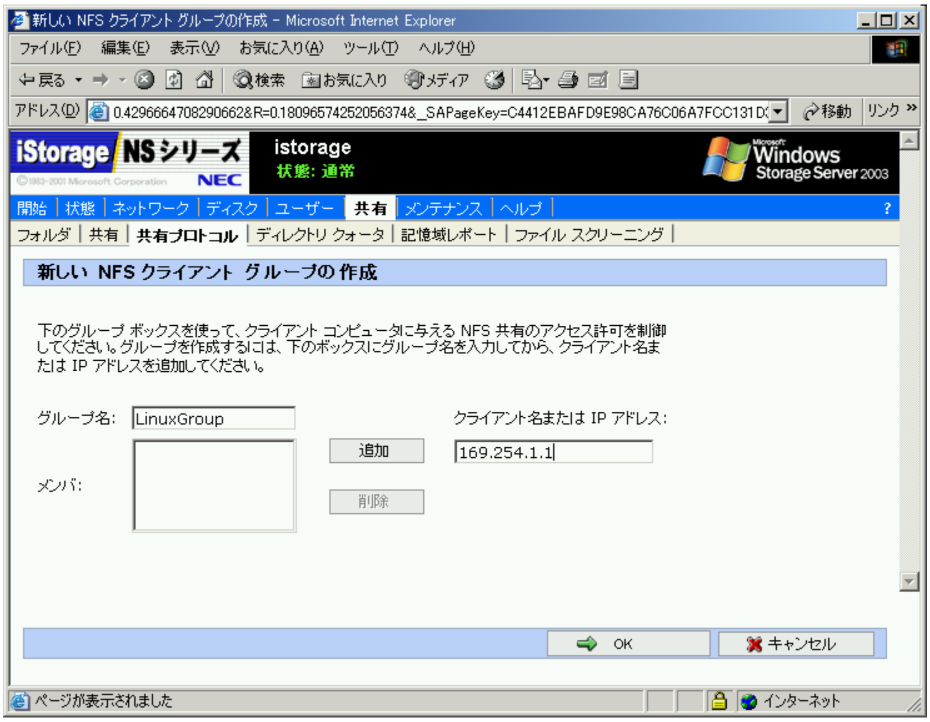
8.4　NFSのアクセス制御

NFS による共有内のフォルダ、ファイルへのアクセス制御には、UNIX の標準的なユーザー／グループに対するアクセス制御の他に、クライアント毎のアクセス制御があります。

クライアント毎のアクセスの制御では、公開する共有にアクセス可能なクライアントをマシン名または IP アドレスで指定し、それらのクライアントに対して、読み取りだけを許可するのか、読み取りと書き込みを許可するのかを指定します。この時、指定するクライアントとして iStorage NS ではクライアントグループという概念を定義し、そのグループに対してアクセス権を与えることができます。クライアントをグループ化する事で、SMB でユーザーのグループに対してアクセス権を付与して木目細かなアクセス制御ができるのと同様に NFS でも細かなアクセス制御を行う事ができます。クライアントグループの設定は以下の手順で行います。

8.4.1　クライアントグループの設定

1. WebUI の[共有]→[共有プロトコル]をクリックします。
2. [NFS]を選び[プロパティ]を選択します。
3. [NFS]ページで[クライアントグループ]を選択します。
4. [新規]でグループ名を指定し、グループ化するクライアントのコンピュータ名または IP アドレスを指定してメンバに[追加]します。
5. メンバを追加後、[OK]ボタンをクリックします。

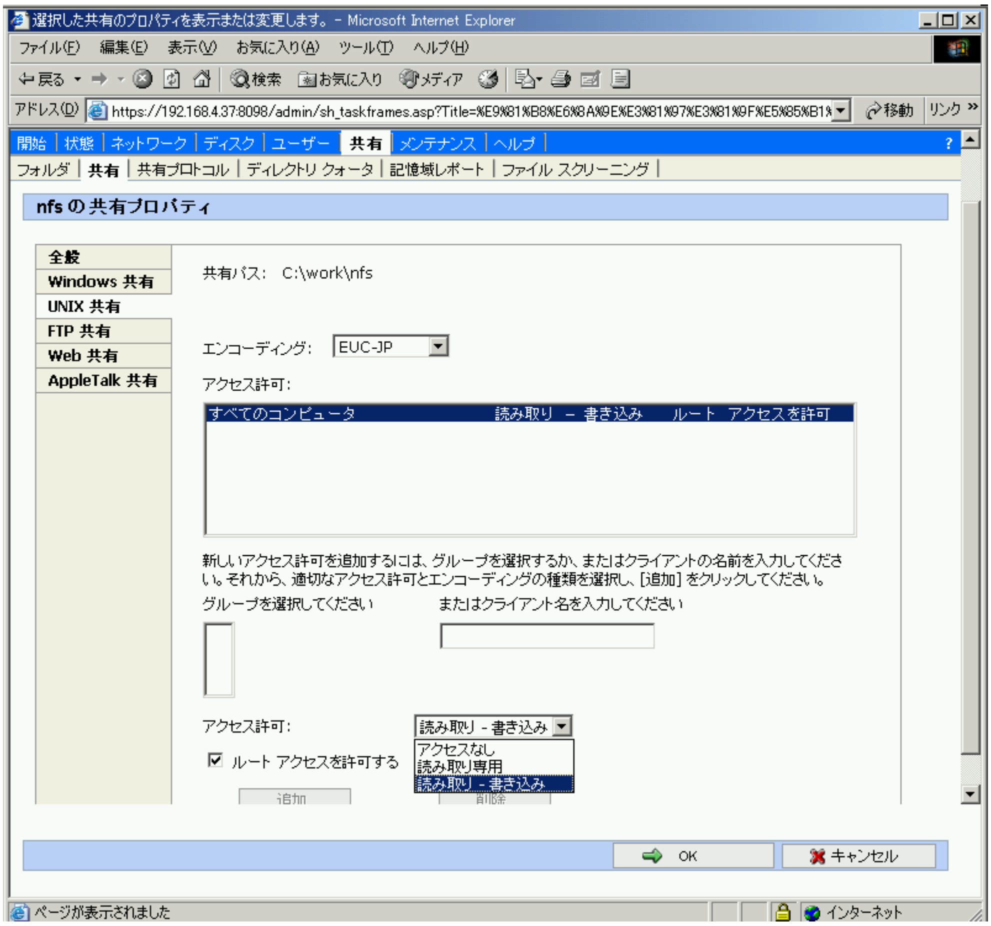


図．NFS クライアントグループの設定

8.4.2　NFS共有のアクセス権の設定

NFS による共有のアクセス権の設定は以下の手順で設定します。

1. WebUI の[共有]→[共有]をクリックします。
2. 設定する共有名を選択し、画面右タスク一覧から[プロパティ]をクリックし、[共有プロパティ]画面を表示します。
3. 画面左の一覧から[NFS 共有]をクリックし、画面を表示します。
4. 画面にあるとおり UNIX のコンピュータ名または IP を入れ[追加]ボタンを押します。
5. [アクセスの種類]を設定し、[OK]ボタンを押します。



図．NFS 共有のアクセス権設定

> root ユーザのマッピングを行っている場合は、アクセスの種類で[読み取り専用＋ルート]または「読み取り － 書き込み＋ルート」を選択しください。

8.4.3 NFSアクセス権に関する注意事項

- 既定では、すべてのマシンが NFS 共有に読み取り専用でアクセスできます。WebUI から NFS 共有に別のマシンまたはグループを追加し、同一種のアクセス設定を[ALL MACHINES] と追加したマシンまたはグループに行った場合、[ALL MACHINES] を [No Access] に自動的に設定します。WebUI では即座にこれが表示されないこともあり、この結果を確認するには、ユーザーは一旦このページから出て、戻ってくる必要がある場合もあります。
- すでにマウントされている状態でNFS共有のプロパティのEUC - JPエンコーディングを有効にした場合は、一度アンマウントし、再度マウントしてください。
- NFS共有の設定を行った場合、すべてのマシンは読み取り専用のみでアクセス出来ます。書き込み等を行う場合は、必要に応じてアクセスの種類を変更してください。
- NFSクライアントグループはマルチバイト文字を使用したグループ名はWebUIからは作成できません。作成する場合は以下の手順にて行ってください。
  (1) WebUIの[メンテナンス]—[リモートデスクトップ]をクリックします。
  (2) ログオン画面が表示されたら、管理者のユーザー名、パスワードを入力し、ログオンします。
  (3) 管理者メニューより [Services for UNIX Administration]を起動し、[Server for NFS]の[Client Groups]タブにて設定を行います。
  (4) プログラムを終了し、リモートデスクトップ画面をログオフします。
- NFS共有では共有名にDBCS文字は使用できません。
- LANケーブルを抜いている状態で、iStorage NSを再起動すると、User Name Mappingサービスが起動に失敗し、イベントログには以下のようなエラーが表示されます。

  「The User Name Mapping service hung on starting」

  User Name Mappingサービスを起動させる場合はLANケーブル接続した状態でサービスを起動してください。

NFSアクセス

・ NFSクライアントとしてHP-UＸを使用する場合は以下の設定を行ってください。

(1) WebUIの[メンテナンス] - [リモートデスクトップ]をクリックします。

(2) ログオン画面が表示されたら、管理者のユーザー名、パスワードを入力し、ログオンします。

(3) レジストリエディタを開き、以下のレジストリの値を変更します。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥NfsSvr¥NlmNsm¥EnableSMBLocking

" 1 "(デフォルト)から" 0 "に変更します。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥NfsSvr¥Parameters¥SecureHandleLevel

" 6 "(デフォルト)から" 5 "に変更します。

(4) 管理者メニューより[サービス]を起動し、[Server for NFS]サービスを再起動します。

(5) リモートデスクトップをログオフします。

8.4.4 Write Cacheの設定の変更手順

「NFS Write Cache」(出荷時は未設定)を設定することで NFS パフォーマンスをさらに高めることが可能です。

注意 :「NFS Write Cache」 の設定される際は、電源の瞬断などが発生した際に完全なデータの保証を約束できない場合があります。「 NFS Write Cache 」を設定する際は、無停電電源装置（UPS）などの電源装置を利用して、安定した電源の供給ができるシステムを構築することをお勧めします。また、UPS を利用せず、データの保全性を重視したい場合は、ディスクアクセス性能は若干、低下しますが、「NFS Write Cache」に使用せず、出荷時の設定にて運用されることをお勧めします。

1. WebUI の[メンテナンス]→[リモートデスクトップ]をクリックします。
2. 管理者権限のあるアカウントを使用してログオンします。
3. 管理者メニューから[NFS Write キャッシュの設定]を起動します。
4. [NFS Write キャッシュ]を使用するにチェックを入れ、OK をクリックします。
5. 管理者メニューから[サービス]を起動します。
6. Server for NFS サービスの再起動を行います。（[NFS Write Cache]が有効となります。）
7. リモートデスクトップからログオフします。

8.5 UNIX環境へのiStorage NS導入について

8.5.1 NFSによる共有について

iStorage NS では、SFU(Services for UNIX)という機能を用いて、UNIX クライアントからのアクセス許可(NFS 共有)を実現しています。SFU とは、Windows と既存の UNIX 環境を容易に統合できるようにするための機能です。

iStorage NS では、SFU の以下のコンポーネントをサポートします。

- Server for NFS : ネットワーク上の UNIXクライアントから Windowsのリソースに NFS 経由でアクセスすることができます。
- Server for NFS Authentication : Server for NFSのファイルにアクセスする際のユーザー認証サービスを実行できます。
- User Name Mapping : WindowsとUNIXでのユーザー名を関連付けます。
- Server for NIS : Windowsのドメイン コントローラをプライマリNISサーバーとして動作させることができます。これにより、NISドメインがWindows のドメインと統合され、管理者はActive Directoryを使用して両方のドメインを管理できます。

8.5.2 iStorage NS導入時のネットワーク環境について

iStorage NS 導入時のネットワーク環境として以下の４つの場合が想定されます。導入時の環境イメージと導入後の環境イメージをそれぞれ説明していきます。

- Windowsドメイン環境でNISサーバを使用している場合
- Windowsドメイン環境でNISサーバを使用していない場合
- ワークグループ環境でNISサーバを使用している場合
- ワークグループ環境でNISサーバを使用していない場合

既存のネットワーク環境でドメインコントローラを使用している場合、iStorage NS 導入時に必要に応じてドメインコントローラにコンポーネントをインストールする必要があります。既存のネットワーク環境とコンポーネントの対応を以下の表に示します。

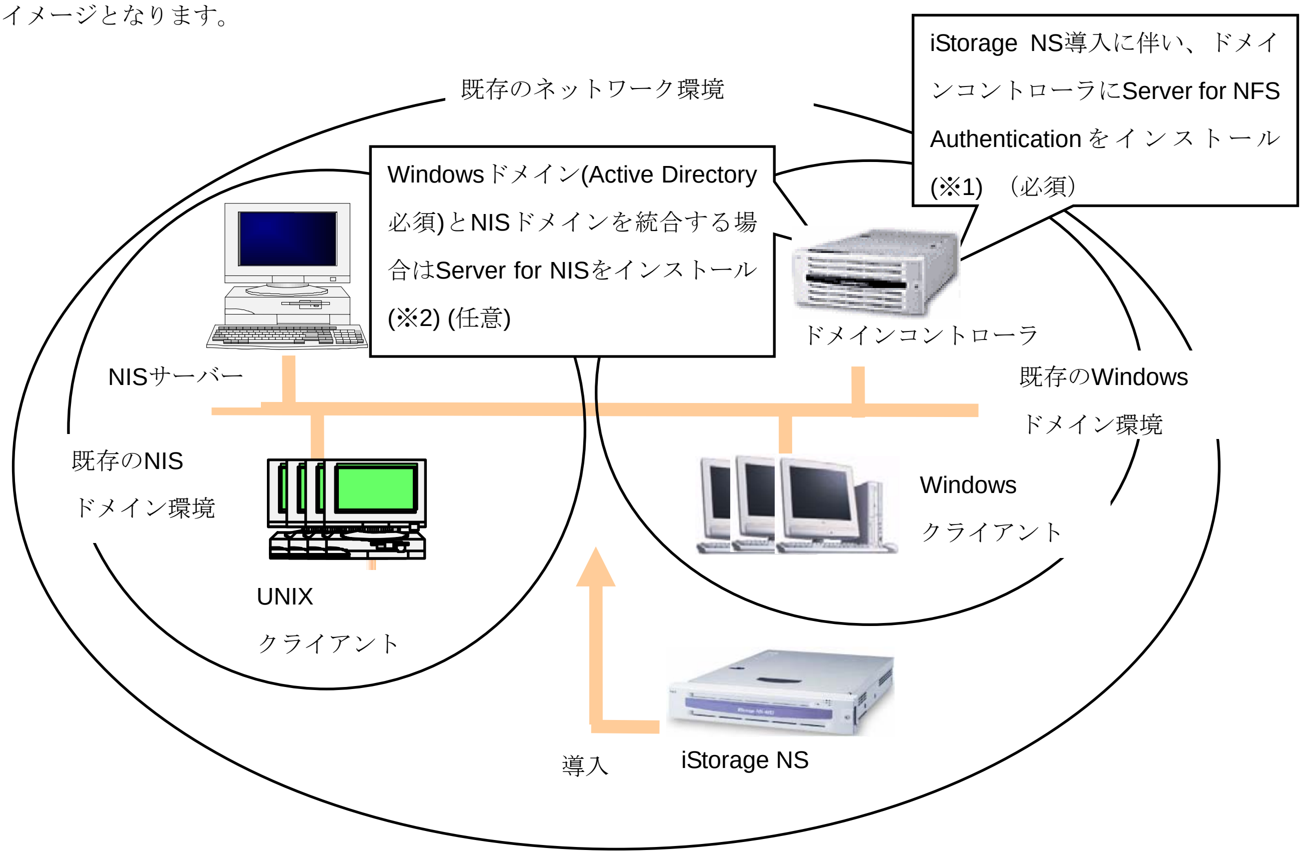
コンポーネント 既存ネットワーク環境	必須コンポーネント	任意コンポーネント
ドメイン環境 NISサーバを使用	Server for NFS Authentication	Server for NIS (Active Directory必須)
ドメイン環境 NISサーバを未使用	Server for NFS Authentication	特になし
ワークグループ環境 NISサーバを使用	特になし	特になし
ワークグループ環境 NISサーバを未使用	特になし	特になし

インストールが必要なコンポーネントにつきましては、付属のEXPRESSBUILDER (SE)CD-ROMのSfu30またはSfu35よりインストールすることができます。

8.5.3　Windowsドメイン環境の場合

8.5.3.1　WindowsドメインC環境でNISサーバを使用している場合

Windows ドメイン環境で NIS サーバを使用している場合に、iStorage NS を導入した場合以下のようなイメージとなります。



1　NFSユーザの認証にドメイン アカウントが使用される場合（Server for NFSのユーザーがWindowsドメイン ユーザーにマップされている場合）は、すべての認証を行うコンピュータ（ドメイン コントローラおよびバックアップ ドメイン コントローラ）に[Services for UNIX Authentication]をインストールする必要があります。

２　[Server for NIS]をドメイン コントローラにインストールよることにより、NISドメインがWindows のドメインと統合され、Active Directoryを使用して両方のドメインを管理できます。これによりシステム管理者はユーザー情報、グループ情報といったUNIX、Windowsの共通情報、またUNIXのみで使用可能なNIS情報もWindows側のみで管理出来るようになります。また、[Server for NIS]の[NIS Server Migration]機能を使用することにより、既存のNIS情報を容易に移行することができます。

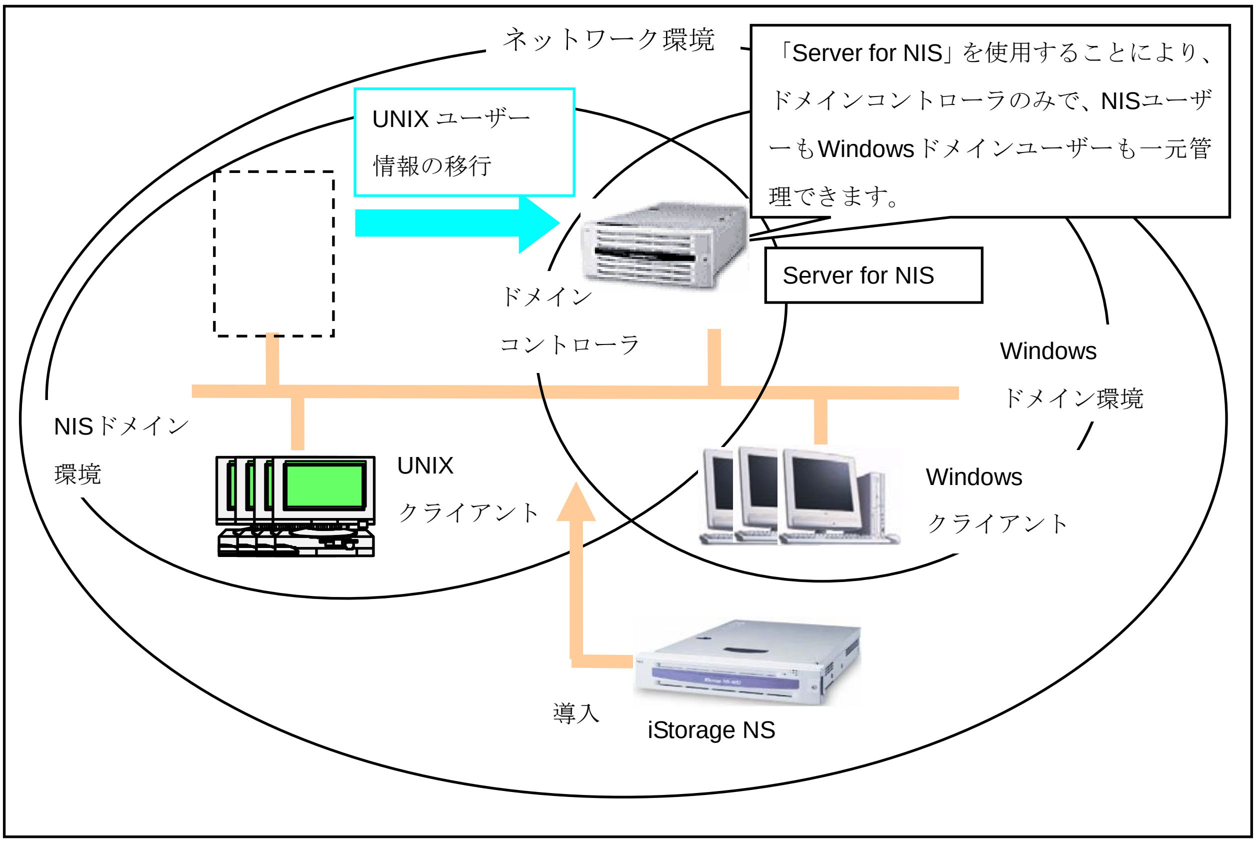
[Server for NIS]を使用するメリット

NIS ユーザーを NIS サーバーにて、また、Windows ドメインユーザーをドメインコントローラで管理している場合、システム管理者はユーザー情報の管理を両コントローラに対し行わなければならず、システム管理者の負担が大きくなります。

そこで、[Server for NIS]を使用することで、ドメインコントローラより、NIS ユーザーや Windows ドメインユーザーが一元管理できるため、システム管理者の負担が大幅に軽減できます。例えば、ユーザー登録時、ドメインコントローラにてユーザーを登録することにより、そのユーザーを Windows ドメインでも NIS ドメインでも使用することが出来ます。また、既存の NIS ユーザーを Windows ドメインユーザーとして、既存の Windows ドメインユーザーを NIS ユーザーとして容易に使用することも出来ます。

以下にドメインコントローラへ server for NIS を導入した場合の環境イメージを示します。

- ドメインコントローラへServer for NISをインストールした場合のネットワーク環境イメージ

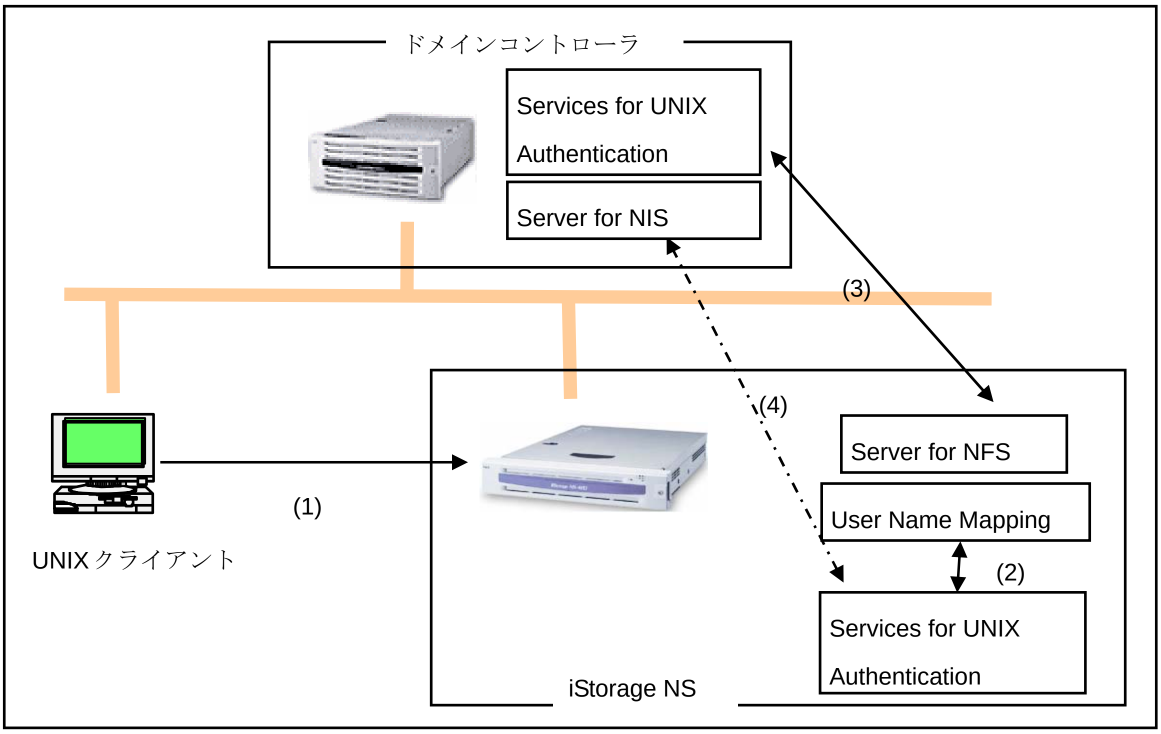


8.5.3.2 iStorage NS 導入後のUNIXクライアントからのアクセス(ドメイン コントローラにServer for NISをインストールした場合)

UNIX クライアントから iStorage NS へアクセスがあった場合、以下のような順序により、ユーザー情報を取得し、ユーザーのアクセスを制御します。

- UNIXクライアントからアクセス時の流れ
  (1) UNIXクライアントからドメインへアクセスします。
  (2) アクセスしたUNIXユーザーの情報を基にServer for NFSがUser Name MappingよりWindowsユーザー情報を取得します。
  (3) Server for NFSがドメインコントローラのServices for UNIX AuthenticationよりWindowsユーザーのセキュリティ情報を取得し、ドメインへログオンします。

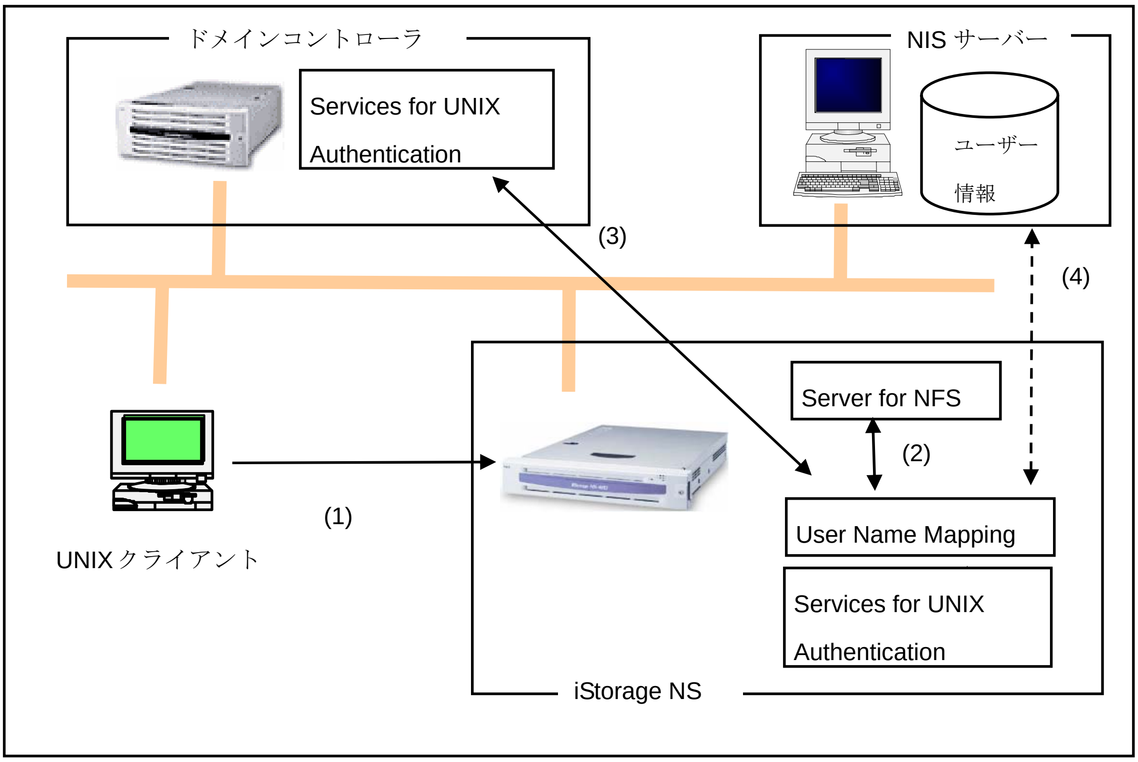
- User Name MappingによるWindowsユーザー情報取得
  (4) Server for NISよりユーザー情報を定期的に取得します。



8.5.3.3 iStorage NS 導入後のUNIXクライアントからのアクセス(既存のNISサーバーを使用する場合)

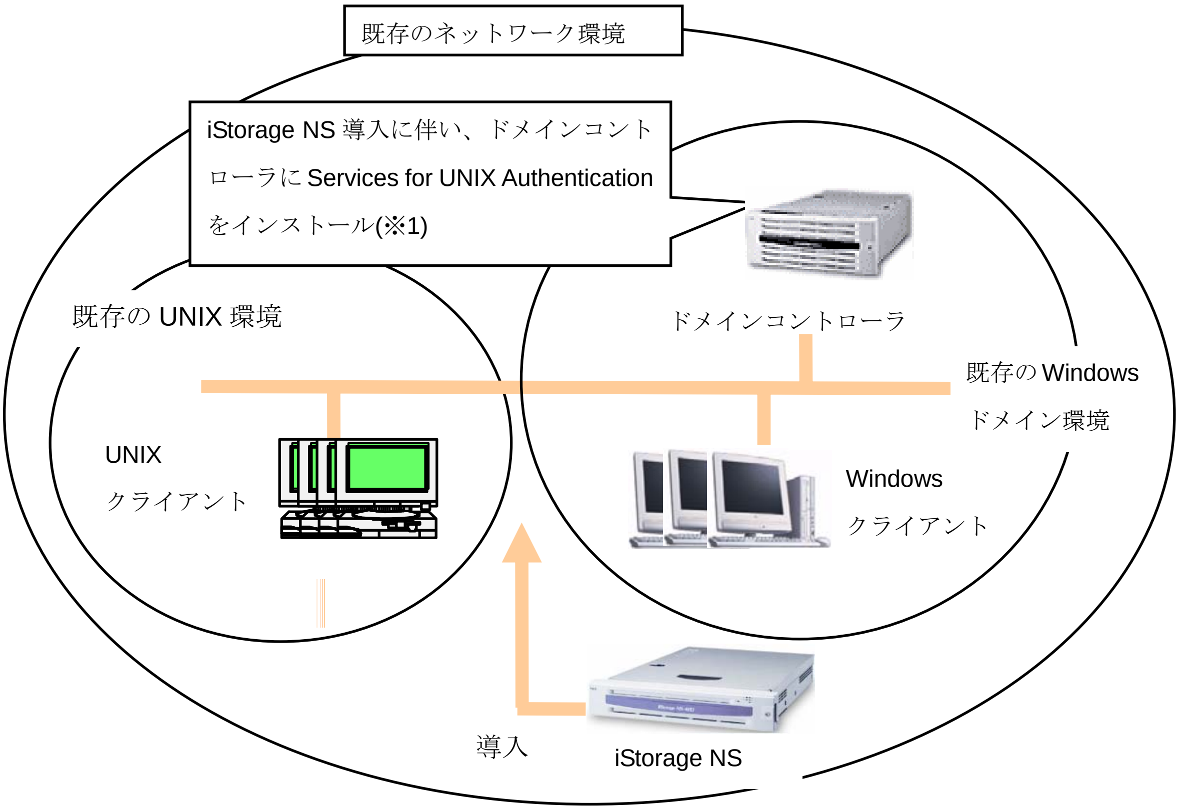
UNIX クライアントから iStorage NS へアクセスがあった場合、以下のような順序により、ユーザー情報を取得し、ユーザーのアクセスを制御します。

- UNIXクライアントからアクセス時の流れ
  (1) UNIXクライアントからドメインへアクセスします。
  (2) アクセスしたUNIXユーザーの情報を基にServer for NFSがUser Name MappingよりWindowsユーザー情報を取得します。
  (3) Server for NFSがドメインコントローラのServices for UNIX AuthenticationよりWindowsユーザーのセキュリティ情報を取得し、ドメインへログオンします。
-
- User Name Mappingによるユーザー情報取得
  (4) NISサーバーよりユーザー情報を定期的に取得します。



8.5.4　Windowsドメイン環境でNISサーバを使用していない場合

Windows ドメイン環境で NIS サーバを使用していない場合に、iStorage NS を導入した場合以下のようなイメージとなります。

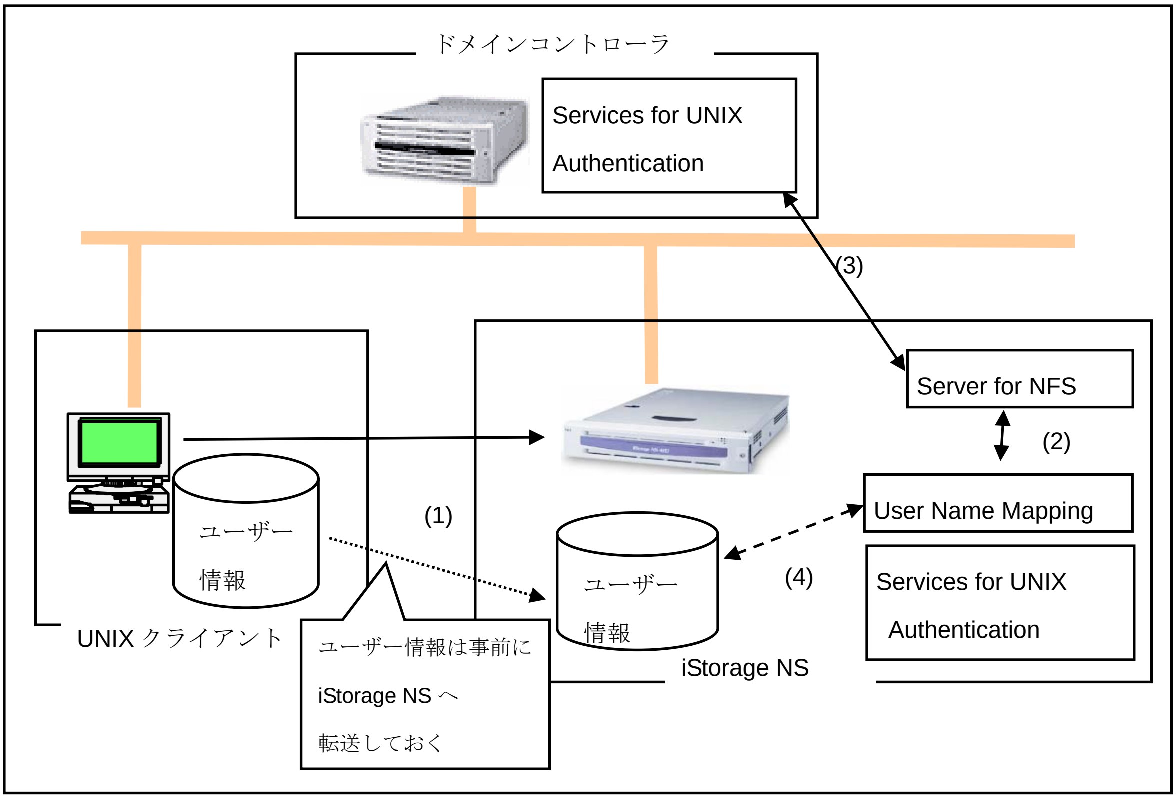


1　NFSユーザーの認証にドメイン アカウントが使用される場合（Server for NFSのユーザーがWindowsドメイン ユーザーにマップされている場合）は、すべての認証を行うコンピュータ（ドメイン コントローラおよびバックアップ ドメイン コントローラ）にServices for UNIX Authenticationをインストールする必要があります。

8.5.4.1　　iStorage NS 導入後のUNIXクライアントからのアクセス

UNIX クライアントから iStorage NS へアクセスがあった場合、以下のような順序により、ユーザー情報を取得し、ユーザーのアクセスを制御します。

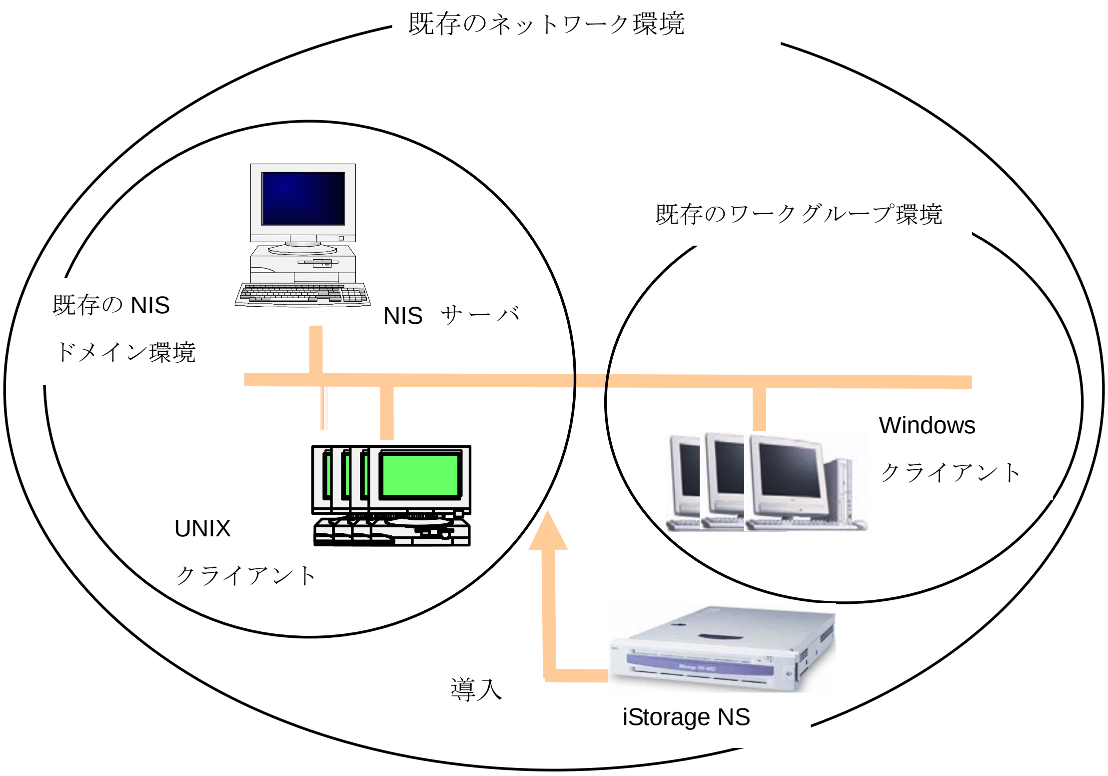
- UNIXクライアントからアクセス時の流れ
  (1) UNIXクライアントからドメインへアクセスします。
  (2) アクセスしたUNIXユーザーの情報を基にServer for NFSがUser Name MappingよりWindowsユーザー情報を取得します。
  (3) Server for NFSがServices for UNIX AuthenticationよりWindowsユーザーのセキュリティ情報を取得し、iStorage NSへログオンします。
-
- User Name Mappingによるユーザー情報取得
  (4) passwdファイル、groupファイルよりユーザー情報を取得します。
  ※ 但し、ユーザー情報ファイルは事前にUNIXクイアントからiSorage NSの任意のディレクトリへ転送しておく必要があります。



8.6　ワークグループ環境の場合

8.6.1　ワークグループ環境でNISサーバを使用している場合

ワークグループ環境で NIS サーバを使用している場合に、iStorage NS を導入した場合以下のようなイメージとなります。



8.6.1.1 iStorage NS 導入後のUNIXクライアントからのアクセス

UNIX クライアントから iStorage NS へアクセスがあった場合、以下のような順序により、ユーザー情報を取得し、ユーザーのアクセスを制御します。

- UNIXクライアントからアクセス時の流れ

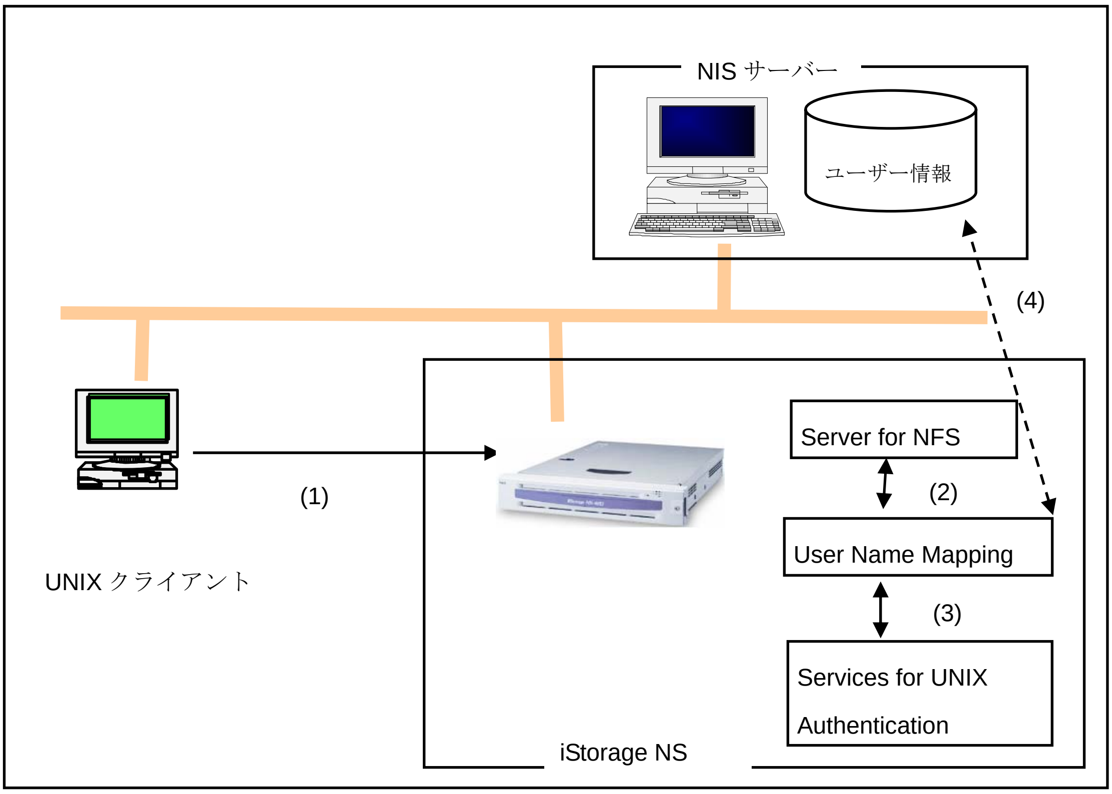
  (1) UNIXクライアントからiStorage NSへアクセスします。

  (2) アクセスしたUNIXユーザーの情報を元にServer for NFSがUser Name MappingよりWindowsユーザー情報を取得します。

  (3) Server for NFSがServices for UNIX AuthenticationよりWindowsユーザーのセキュリティ情報を取得し、iStorage NSへログオンします。

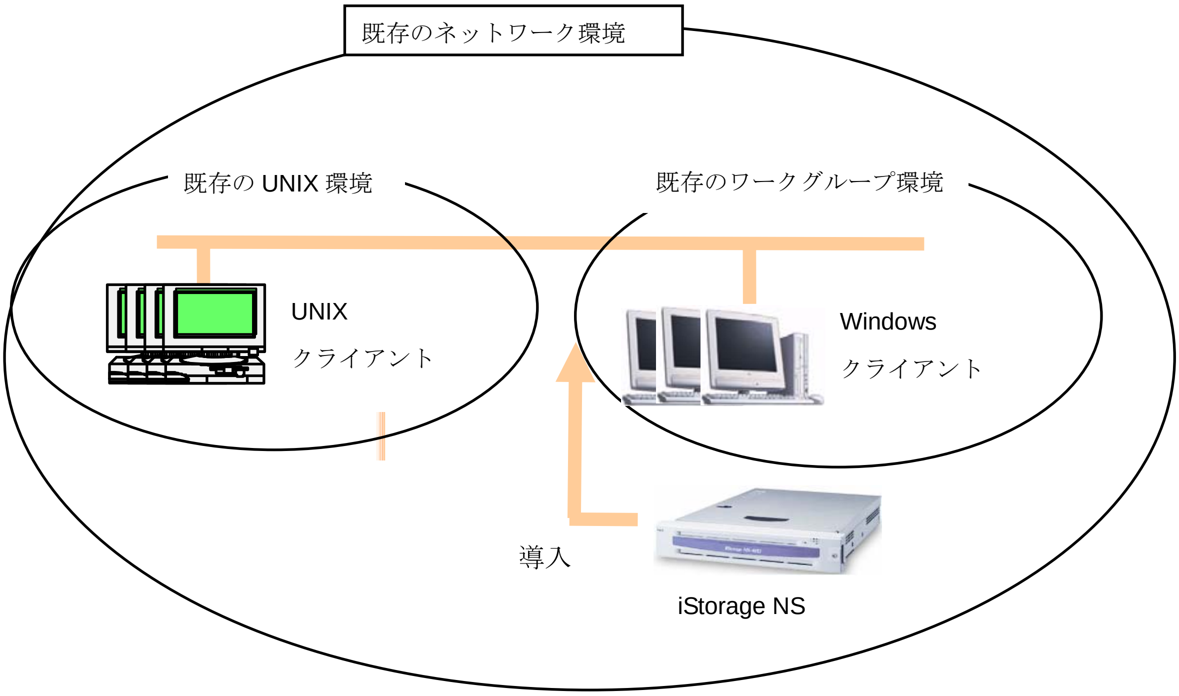
- User Name Mappingによるユーザー情報取得

  (4) NISサーバーよりユーザー情報を定期的に取得します。



8.6.2　ワークグループ環境でNISサーバを使用していない場合

ワークグループ環境で NIS サーバを使用していない場合に、iStorage NS を導入した場合以下のようなイメージとなります。

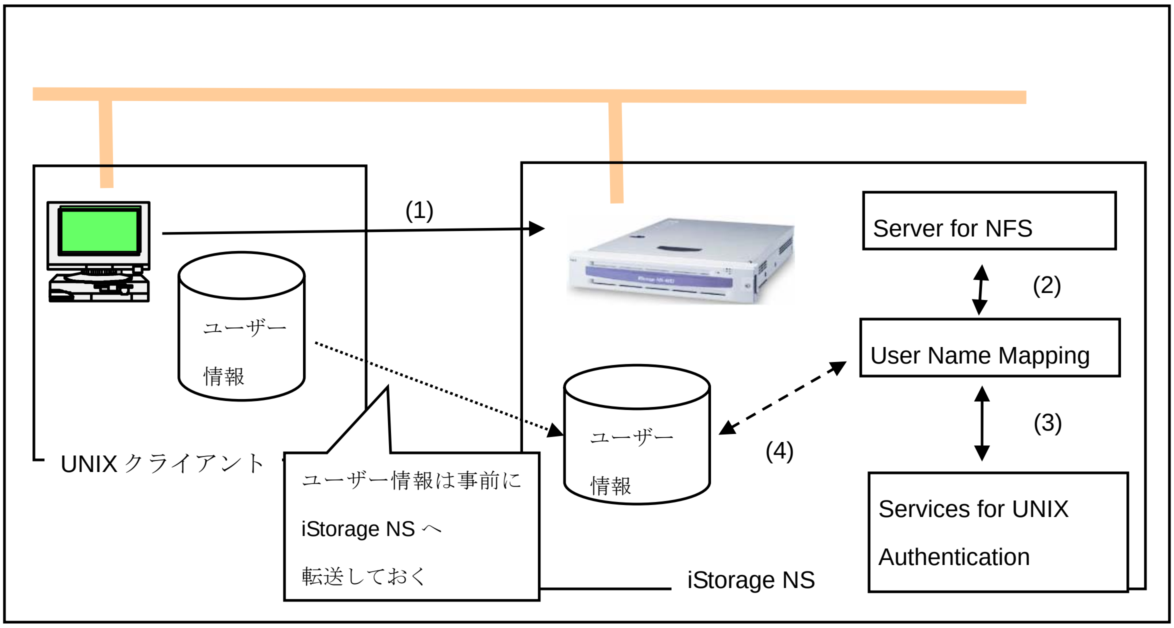


8.6.2.1 iStorage NS 導入後のUNIXクライアントからのアクセス

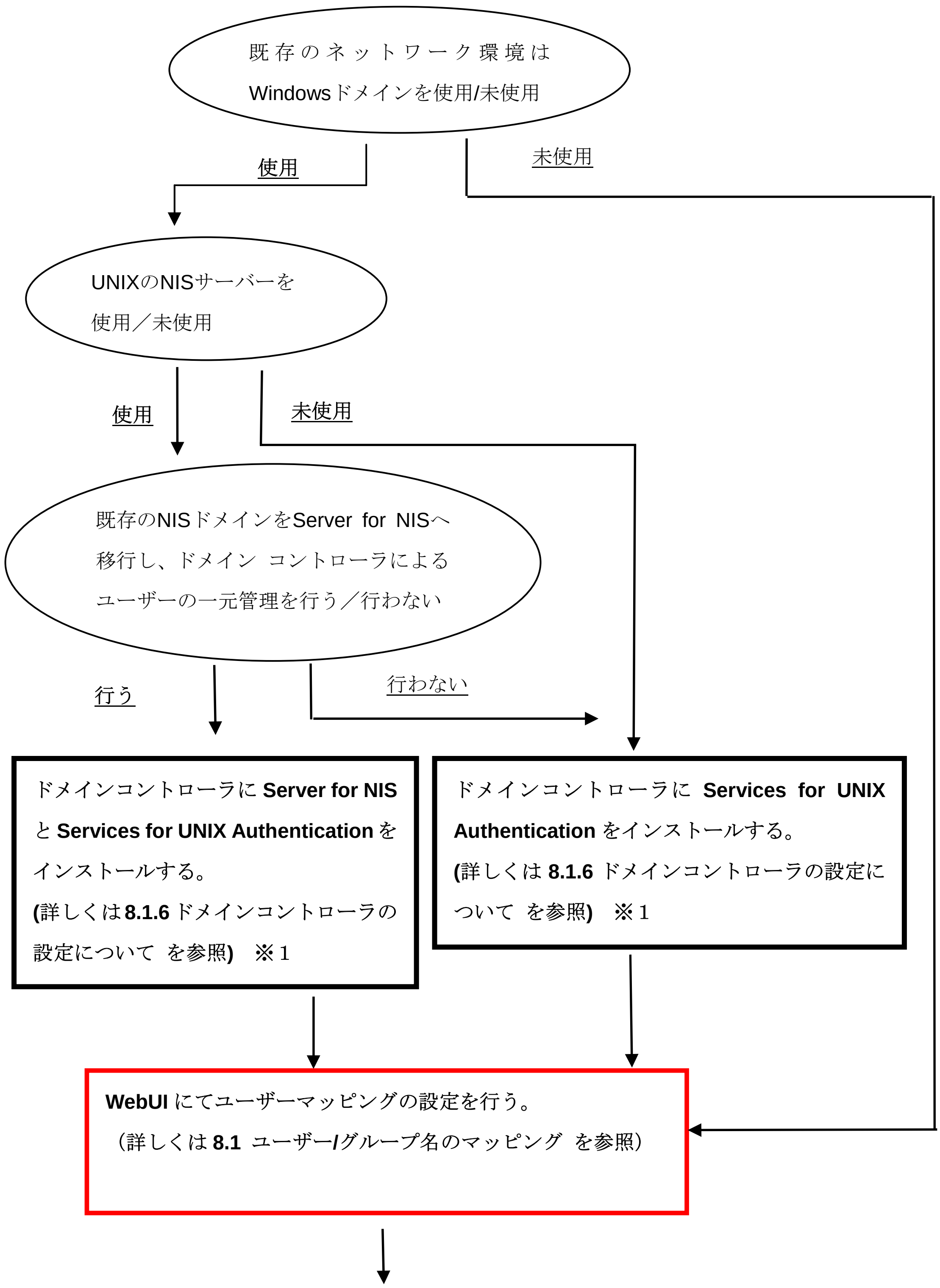
UNIX クライアントから iStorage NS へアクセスがあった場合、以下のような順序により、ユーザ情報を取得し、ユーザのアクセスを制御します。

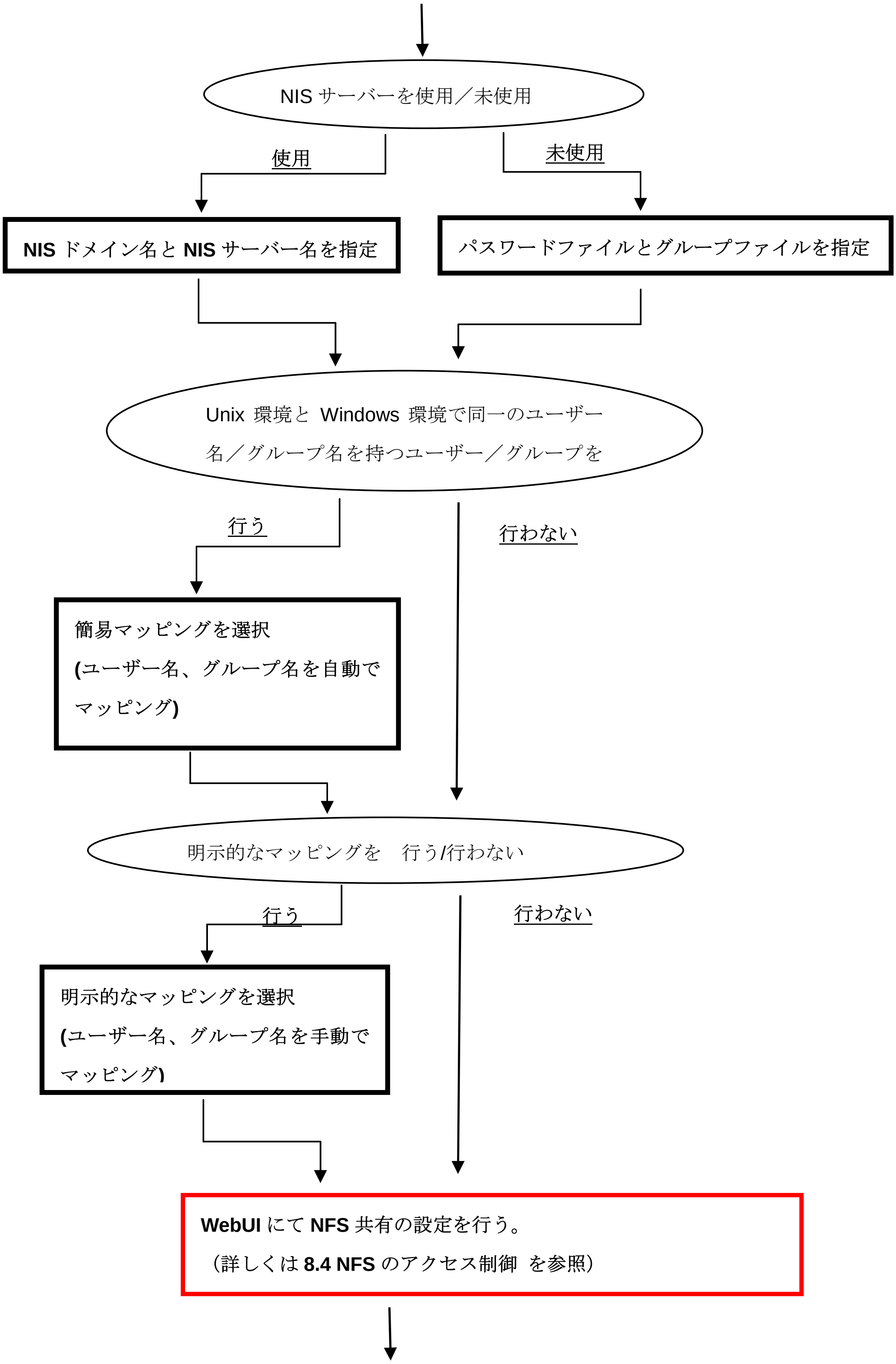
- UNIXクライアントからアクセス時の流れ
  (1) UNIXクライアントからiStorage NSへアクセスします。
  (2) アクセスしたUNIXユーザーの情報を元にServer for NFSがUser Name MappingよりWindowsユーザー情報を取得します。
  (3) Server for NFSがServices for UNIX AuthenticationよりWindowsユーザーのセキュリティ情報を取得し、iStorage NSへログオンします。

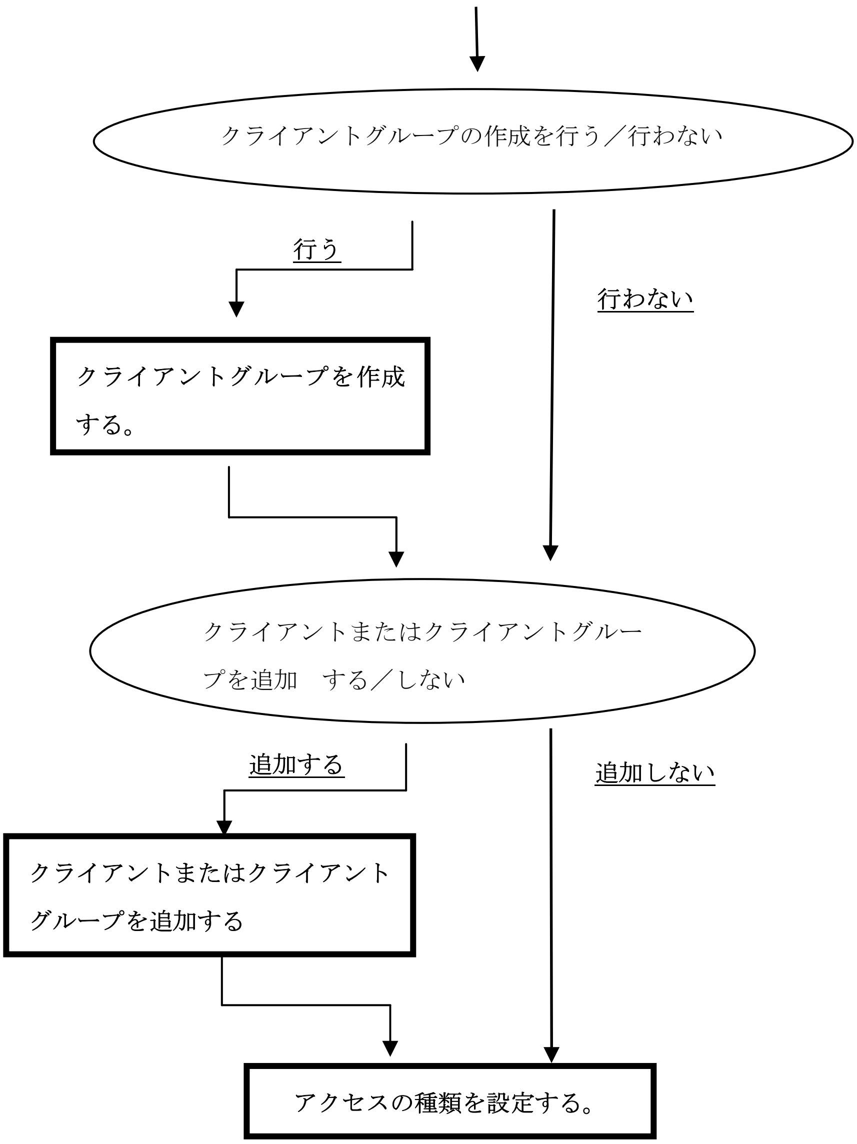
- User Name Mappingによるユーザー情報取得
  (4) passwdファイル、groupファイルよりユーザー情報を取得します。
  但し、ユーザー情報ファイルは事前にUNIXクイアントからiSorage NSの任意のディレクトリへ転送しておく必要があります。



8.6.3 iStorage NS導入時のNFS共有 設定の流れ




NIS サーバーを使用／未使用
使用
未使用
NIS ドメイン名と NIS サーバー名を指定
パスワードファイルとグループファイルを指定
Unix 環境と Windows 環境で同一のユーザー名／グループ名を持つユーザー／グループを
行う
行わない
簡易マッピングを選択
(ユーザー名、グループ名を自動でマッピング)
明示的なマッピングを　行う/行わない
行う
行わない
明示的なマッピングを選択
(ユーザー名、グループ名を手動でマッピング)
WebUI にて NFS 共有の設定を行う。
（詳しくは 8.4 NFS のアクセス制御 を参照）


クライアントグループの作成を行う／行わない
行う
行わない
クライアントグループを作成する。
クライアントまたはクライアントグループを追加　する／しない
追加する
追加しない
クライアントまたはクライアントグループを追加する
アクセスの種類を設定する。

8.6.4　　トラブルシューティング

- ユーザーマッピングが正常に反映されない。
  対策：ユーザーマッピングの設定を確認してください。(詳しくは 8.1 ユーザー/グループ名のマッピングを参照して下さい。)
  またWindowsドメインを使用している場合は、すべてのドメインコントローラにServices for UNIX Authenticationをインストールする必要があります。(詳しくは 8.1.6.3　ドメインコントローラの設定を参照して下さい。)

- Windows環境からファイルを作成するとマッピング情報が反映されない。
  対策：マッピングの設定を確認してください。 (詳しくは 8.1.4 Windows環境からファイルを作成する場合について を参照して下さい。)

- rootユーザーが使用できない。
  対策：iStorage NSでrootユーザーを使用するには、アクセスの種類で[読み取り専用 ＋ルート]または[読み取り-書き込み ＋ルート]を選択しておく必要があります。(詳しくは 8.1.2 rootのマッピングについて　を参照して下さい。)

- ファイルの書き込みが行えない。
  対策：NFS共有のアクセス権が[読み取り専用](デフォルト設定)になっている可能性があります。必要に応じてNFS共有のアクセスの種類を変更してください。(詳しくは 8.４.2 NFS共有のアクセス権の設定 を参照して下さい。)
  また、mountコマンドのオプションでro(Read Only)が設定されている可能性があります。mountコマンドのオプション設定を確認してください。

- UNIXクライアントにて、NFS共有フォルダで lsコマンド等を実行すると、フォルダやファイルの所有者が nobody と表示される。
  対策：パスワードの有効期限が切れています。パスワードを設定してください。

9 FTP/HTTPアクセス

iStorage NS からクライアントへ公開する“共有”を設定します。クライアントがアクセスするための共有名と、その共有を iStorage NS 内のどのフォルダに作成するかを指定します。

9.1 FTP／HTTPによる共有

iStorage NS 内に新たに共有を作成するには、以下の手順で行います。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します。
2. WebUI の[共有]→[共有]をクリックします
3. タスクの[新規]をクリックします
4. 共有名、共有パスなどを設定し、[FTP]または[Web（HTTP）]を選択します
5. [FTP 共有]または[Web 共有]タブをクリックし、設定を行った後、[OK]ボタンをクリックします。

FTP クライアントや HTTP クライアントからファイルアクセスするための共有を設定します。FTP での共有では、アクセスログを採取する事ができます。ログはデフォルトでは iStorage NS の C:¥Windows¥System32¥LogFiles¥MSFTPSVC1¥ 配下に作成されます。

また、[共有]→[共有プロトコル]→[FTP]の[プロパティ]から、匿名アクセスの設定や FTP アクセス時の開始メッセージ・終了メッセージを設定できます。

HTTP による共有の設定では、ネットワークインタフェースを複数持ちそれぞれに IP アドレスが割り当てられている場合に、全ての IP アドレスで HTTP による共有へのアクセスを許すか、１つの IP アドレスしか許さないかの設定やポート番号の設定を行います。

共有を設定する際は、設定した共有に対するアクセス権も必ず設定する事をお勧めします。アクセス権に関しては、[FTP/HTTP のアクセス制御]の項を参照して下さい。

HTTP 共有の注意

- WebUI のリモートデスクトップを使って iStorage NS に接続後、インターネットインフォメーションサービス（IIS）マネージャを使用して、 HTTP 共有を作成する場合、この新規共有は、WebUI を使用して新規共有を作成しない限り、[共有] ページ上には表示されません。これは、新規共有が WebUI を使用して作成されたときのみに default.htm ページが生成されるためです。共有は WebUI から作成してください。
- WebUI の[共有]→[共有のプロパティ]をクリックし[次の IP のみ]を選択した場合にも、「0.0.0.0」を選択すると HTTP 共有フォルダへのアクセスができなくなりますので選択しないでください。

9.2　FTP／HTTPクライアントからのアクセス

FTP や HTTP で iStorage NS 上のファイルへアクセスするには、FTP クライアントソフトウェアや HTTP クライアントソフトウェアを使用します。FTP や HTTP でのファイルアクセスの方法は、各ソフトウェアの使用方法に従って下さい。例えば、Windows クライアントで FTP コマンドを実行するには、コマンドプロンプトを開き、" ftp ＜iStorage NS の URL＞" と入力することで ftp アクセスが可能です。　また、Internet Explorer 等で iStorage NS の URL（ex. http://＜iStorage NS のコンピュータ名＞.＜iStorage NS が含まれるドメイン名＞/[：＜ポート番号＞]）へアクセスする事で HTTP により公開した共有へアクセスする事が可能です。既定の HTTP 共有のポートは 80 です。既定ポートが管理者により変更されていない限り、HTTP 共有に接続する際には、ポートを指定する必要はありません。

9.2.1　WebDAVについて

WebDAV については、IIS のヘルプを参照してください。

9.3　FTP／HTTPのアクセス制御

ユーザーや複数のユーザーをまとめたグループに対して各共有へのアクセスを制限する事で、セキュリティを保ったファイルアクセスの管理を行います。アクセス制御によって、必要なユーザーだけにファイルをアクセス可能にし、不必要なユーザーからのアクセスを禁止することで、不正な参照や書き換え削除を防止します。

FTP と HTTP での共有へのアクセスの制御は、認証された全てのユーザーに対して、読み取りを許すか否か、書き込みを許すか否かのみです。

10 AppleTalkアクセス

iStorage NS から Macintosh クライアントへ公開する“共有”を設定します。クライアントがアクセスするための共有名と、その共有を iStorage NS 内のどのフォルダに作成するかを指定します。工場出荷時にはユーザー領域として使用できる共有を定義していません。新たに共有を定義して使用を開始してください。

> 工場出荷状態では、フォルダ C:¥Microsoft UAM Volume を共有名 Microsoft UAM Volume で AppleTalk 共有しています。この共有はシステムで使用しますので、設定の変更、ユーザーデータの共有領域としての利用、削除等を行わないで下さい。AppleTalk 共有を行う場合は、必ず新規で上記以外の共有を作成してください。

> **iStorage NS14PW** にて Apple Talk を利用する場合、512MB 以上のメモリを搭載してください。また、出荷時はサービスが無効になっていますので、後述の手順に従ってサービスを開始させてください。

AppleTalkアクセス

出荷時、AppleTalk が無効となっている機種(**NS14PW**)において、AppleTalk をご利用になる場合は、以下の手順に従って、サービスを開始させてください。

1. WebUIの[メンテナンス]→[リモートデスクトップ] をクリックし、管理者権限のアカウントを使用してログオンします。
2. [管理者メニュー] より、[サービス] を起動します。
3. [File Server for Macintosh] サービスのプロパティにて、スタートアップの種類を[自動]にして、[開始]ボタンをクリックします。
4. [OK]ボタンをクリックして、プロパティ画面を閉じます。

10.1　フォルダの作成と共有設定

AppleTalk 共有を使用する際の準備

AppleTalk 共有を使用する場合、[ネットワーク]→[インターフェイス]で AppleTalk を使用するアダプタを選択し、タスク欄の[AppleTalk]をクリックして下記の設定を行ってください。

1. [このアダプタで着信 AppleTalk 接続を有効にする]にチェックを入れます。
2. ゾーンを設定している場合は、ここでゾーンを選択します。
3. 上記設定後、OK ボタンをクリックします。

AppleTalk 通信に使用できるアダプタは 1 ポートのみです。

iStorage NS 内に新たに共有を作成するには、以下の手順で行います。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します。
2. WebUI の[共有]→[共有]をクリックします。
3. タスクの[新規]をクリックします。
4. [共有名]と[パス名]を設定して OK をクリックします。
5. [Apple Macintosh]をチェックし、[AppleTalk 共有]をクリックします。
6. 設定を行った後、[OK]ボタンをクリックします。

AppleTalk による共有は、Macintosh クライアントからファイルアクセスするための設定です。設定画面では、

- 共有に一度にアクセスできるユーザー数の制限の指定
- 共有させるボリューム、フォルダへのパスワードの設定
- ユーザーにファイルを読み書きさせるかまたは読み取り専用にさせるかの設定を指定します。

AppleTalk 共有に関する注意

1. MacOS X 以降のクライアントからアクセスする必要があるボリュームには、ボリュームパスワードを設定しないでください。アクセスができなくなります。
2. あるフォルダに AppleTalk 共有と Windows 共有が設定されている状態で、リモートデスクトップ画面を使用してこのフォルダに"everyone"にフルコントロールの権利を設定し、AppleTalk 共有のプロパティを変更して OK をクリックすると、Windows 共有のページが開き、「ユーザーはすでに存在します」というエラーになり共有のページが終了しません。この場合、Windows 共有のプロパティのページには、"everyone"が複数表示されています。いずれかを削除して OK ボタンを押すと正常に終了します。

10.1.1 AppleTalk共有のプロパティ設定

また、[共有]－[共有プロトコル]の AppleTalk プロトコルのプロパティから以下の設定が可能です。

ログオンメッセージ

Mac ユーザーが iStorage NS にログオンしたときに表示されるメッセージを設定できます。省略可能です。

セキュリティ

[ワークステーションにパスワードを保存するのを許可する]にチェックすることで、Mac ユーザーが iStorage NS にアクセスする際のパスワードの保存を許可します。

[認証を有効にする]は、パスワードの認証方法を指定するオプションです。以下の項目が選択できます。

Microsoft のみ. . . MicrosoftUAM によるパスワード認証です。パスワードが暗号化されてネットワークに流れるため、安全性が高いといえます。事前に MicrosoftUAM の組み込みが必要です。（インストールの方法は後ほど説明する[Microsoft UAM のインストールについて]を参照願います。）

Apple のクリアテキスト. . . AppleUAM によるパスワード認証です。パスワードがクリアテキストでネットワークを流れるため、セキュリティのレベルは低くなります。

Apple の暗号化. . . AppleUAM によるパスワード認証です。パスワードが暗号化してネットワークを流れるため、安全性が高いといえます。(MacOS X クライアントからのアクセス、または iStorage NS が WindowsNT4.0 ドメインに参加している環境では未サポートですので選択しないでください。) このオプションを使用する場合、あらかじめ、ローカルセキュリティポリシーで設定が必要です。また、これを有効にする前に設定したユーザー名とパスワードではこの暗号化オプションでログオンできませんので、再度パスワードを設定しなおしてください。（設定については後ほど説明する[セキュリティ（認証方法が Apple 暗号化のとき）]を参照願います）

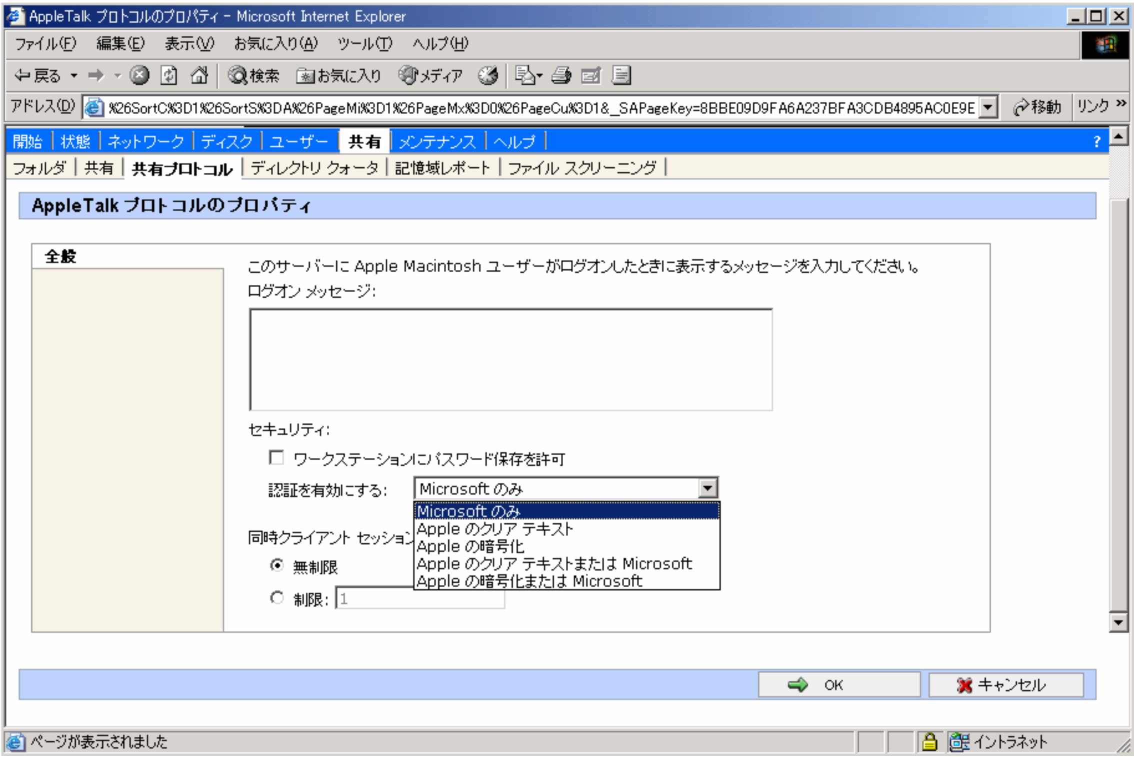
Apple のクリアテキストまたは Micorosoft. . . MacOS 9 以前のクライアントで MicrosoftUAM がインストールされている場合、ログオン時にどちらのユーザー認証を使用するか選択できます。クライアントが MacOS X 以降の場合は、MicrosoftUAM による認証が優先されますので、クリアテキストでの接続には、[Apple クリアテキスト]を選択してください。（MicrosoftUAM のインストールの方法は [Microsoft UAM のインストールについて]を参照願います）

Apple の暗号化または Micorosoft. . .　MacOS 9 以前のクライアントで、MicrosoftUAM がインストールされている場合、ログオン時にどちらのユーザー認証を使用するか選択できます（MacOS X クライアントからのアクセス、または iStorage NS が WindowsNT4.0 ドメインに参加している環境では未サポートです。）MicrosoftUAM を使用する場合は、事前に組み込みが必要です（インストールについては後ほど説明する[Microsoft UAM のインストールについて]を参照願います)。MacOS 9 以前のクライアントが Apple 暗号化を使用する場合は、ローカルセキュリティポリシーで設定が必要です。また、これを有効にする前に設定したユーザー名とパスワードではこの暗号化オプションでログオンできませんので、再度パスワードを設定しなおしてください(設定については後述する[セキュリティ(認証方法が Apple 暗号化のとき)]を参照願います)。

セッション数

無制限. . .　同時接続可能なユーザー数を制限しません。

制　限. . .　同時接続可能なユーザー数を制限できます。



図．AppleTalk 共有のプロパティ

10.1.2 セキュリティ（認証方法がApple暗号化のとき）

クライアントがMacOS X以降またはiStorage NSが参加するドメインがWindowsNT4.0の場合はこの手順は省略してください。

MacOS 9以前のクライアントからApple暗号化を使用し、ドメインユーザーとそのパスワードを使用してファイル共有する場合、以下の設定が必要です。なお、ドメイン環境下でApple暗号化を使用する場合ドメインコントローラには Windows Server 2003 / Windows2000 を使用してください。

Windows Server 2003/Windows2000 ではない場合はワークグループと同様の設定を行ってください。ドメイン／ワークグループ、ドメインコントローラが Windows Server 2003 / Windows2000 かそうでないかにより、設定の方法が異なります。以下では、

- 「ワークグループでの利用」又は「ドメインコントローラがWindows Server 2003 / Windows2000でない環境での利用」の場合
- 「ドメインコントローラがWindows Server 2003 / Windows2000であるドメインでの利用」の場合

に分けて設定方法を記述します。

<u>「ワークグループでの利用」の場合</u>

iStorage NS 上のローカルセキュリティポリシーのパスワードポリシーに以下の設定を行います。尚、下記で設定を有効にする前の既存のユーザーパスワードは保存されていないため有効にした後、ユーザーパスワードを再度入力または変更する必要があります。

1. リモートデスクトップ画面（[メンテナンス]－[リモートデスクトップ]）で、[スタート]→[管理ツール]→[ローカルセキュリティポリシー]を開く。
2. [アカウントポリシー] をダブルクリックし、次に、[パスワードのポリシー] をクリックする。
3. [暗号化を元に戻せる状態でパスワードを保存する] を右クリックし、次に、[プロパティ] をクリックする。
4. [有効] を選択し[OK]をクリックする。

以上で設定は終了です。

「ドメインコントローラが **Windows2000/2003** であるドメインでの利用」の場合

Windows 2000/2003 のドメインコントローラには、ローカルセキュリティポリシー、ドメインセキュリティポリシーとドメインコントローラセキュリティポリシーの 3 つのポリシーがあります。ここでは、ご使用の環境のドメインコントローラ上で、ドメインセキュリティポリシーの設定を行います。ここでは Windows2000 での設定方法です。Windows 2003 の場合はメニュー等が異なる場合があります。

1. ドメインコントローラ上で、[スタート]→[プログラム]→[管理ツール]→[ドメインセキュリティポリシー]を開きます。
2. [アカウントポリシー] をダブルクリックし、次に、[パスワードのポリシー] をクリックします。
3. [暗号化を元に戻せる状態でドメインのすべてのユーザーのパスワードを保存する] を右クリックし、次に、[セキュリティ] をクリックします。
4. [有効] をクリックし[OK]します。

以上で設定は終了です。この設定を iStorage NS に反映させるためにこの設定終了後 WebUI から iStorage NS を再起動させてください。

10.2 Macintoshクライアントからのアクセス

クライアント(MacOS 10.1.5 の場合)からの接続例を以下に示します。

1. 移動メニュー-から[サーバへ接続]を選択する。
2. [AppleTalk]をクリックし、ゾーンを選択する。
3. 表示されたサーバーの一覧から、ログオンするサーバー名を選択して[接続]をクリックする。



4. ユーザー名とパスワードを入力し、[接続]をクリックする。



上の図は認証の方法として[Appleのクリアテキスト]を選択している場合です。

5. 共有設定したボリューム名が表示されるので、選択し、OK ボタンをクリックする。



6. ログオン時のメッセージを設定している場合は、メッセージ画面が表示されるので、OK ボタンをクリックする。（ログオン時のメッセージを設定していない場合は省略されます。）
7. デスクトップに共有名の名前のアイコンが表示されたら（ここでは“test1”）ダブルクリックで開き、中のファイルにアクセスできます。

また、MacOS X 以降のクライアントから、リモートデスクトップによる接続も可能です。
詳細は以下の URL で確認してください。

http://www.microsoft.com/japan/mac/collaboration/rdc/default.asp （2006 年 3 月 29 日現在)

Microsoft UAM のインストールについて

iStorage NS へのユーザー認証で Microsoft UAM を使用する場合は、以下の設定が必要です。

> MacOS 9 以前のクライアントでは、システムフォルダ内の Apple Share Folder に MS UAM 5.0 のアイコンがあれば、以下の設定は必要ありません。
>
> MacOS X 以降のクライアントは以下のファイルがあれば、設定は必要ありません。
>
> Library/Filesystems/AppleShare/Authentication/MicrosoftUAM.uamx

インストール手順

MacOS 9 以前の場合

1. Macintosh クライアントからサーバーに接続します。開くボリュームは[Microsoft UAM Volume]を選択してください。
2. Macintosh クライアントのデスクトップ上に、同名のアイコンが表示されますので、ダブルクリックで開きます。
3. [MS UAM Installer]をダブルクリックし、ウィザードに従ってインストールしてください。
4. インストールが終了したら、デスクトップのハードディスクアイコン（初期値では Macintosh HD）を開き、[システムフォルダ]→[Apple Share Folder]をダブルクリックで開きます。ここに[MS UAM 5.0]というアイコンが作成されていればインストール終了です。

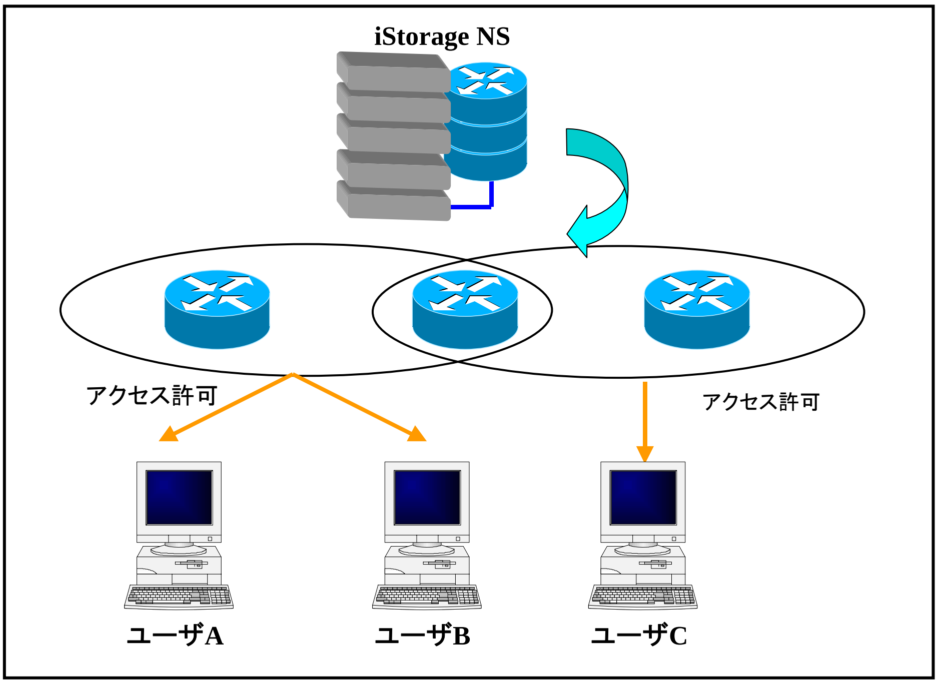
MacOS X 以降の場合

マイクロソフトの Web サイトから、MacOS X 用のモジュールをダウンロードしてください。インストールに関しては、解凍後に作成される ReadMe ファイルに従ってください。

> Macintoshクライアントより iStorage NSに対してファイルコピーが出来なくなった場合、iStorage NSまたはMacintoshクライアントを再起動することで解決できるようになることがあります。

10.3 AppleTalkのアクセス制御

ユーザーや複数のユーザーをまとめたグループに対して各共有へのアクセスを制限する事で、セキュリティを保ったファイルアクセスの管理を行います。アクセス制御によって、必要なユーザーだけにファイルをアクセス可能にし、不必要なユーザーからのアクセスを禁止することで、不正な参照や書き換え、削除を防止します。



図．アクセス制御

AppleTalk での共有へのアクセスの制御では、

- 共有に一度のアクセスできるユーザー数の制限
- 対象の共有に対するパスワード
- ユーザーに対してファイルを読み取り専用とするかどうか

を設定できます。設定は[共有]－[共有]でアクセス権の設定を行う共有にチェックをし、[プロパティ]を選択します。

また、Windows（SMB）共有と同様にユーザー・グループごとに読み取り、実行などのアクセス権を設定することも可能です。この場合、以下の方法で行います。

1. 管理 PC でブラウザを起動し、iStorage NS の WebUI を表示します

2. [メンテナンス]→[リモートデスクトップ]をクリックし、リモートデスクトップ画面を起動します。
3. 管理者権限のアカウントでログオン後、管理者メニューの[コンピュータの管理]を選択します。
4. [コンピュータの管理]が開いたら、左ツリーの[共有フォルダ]をダブルクリックします。
5. [共有フォルダ]配下の[共有]をクリックすると右側のウィンドウにWindowsとMacintoshの共有の一覧が表示されます。
6. セキュリティ設定を行う共有をダブルクリックし、プロパティを開きます。
7. セキュリティタブを開き、必要な設定を行い、OKボタンをクリックして終了します。